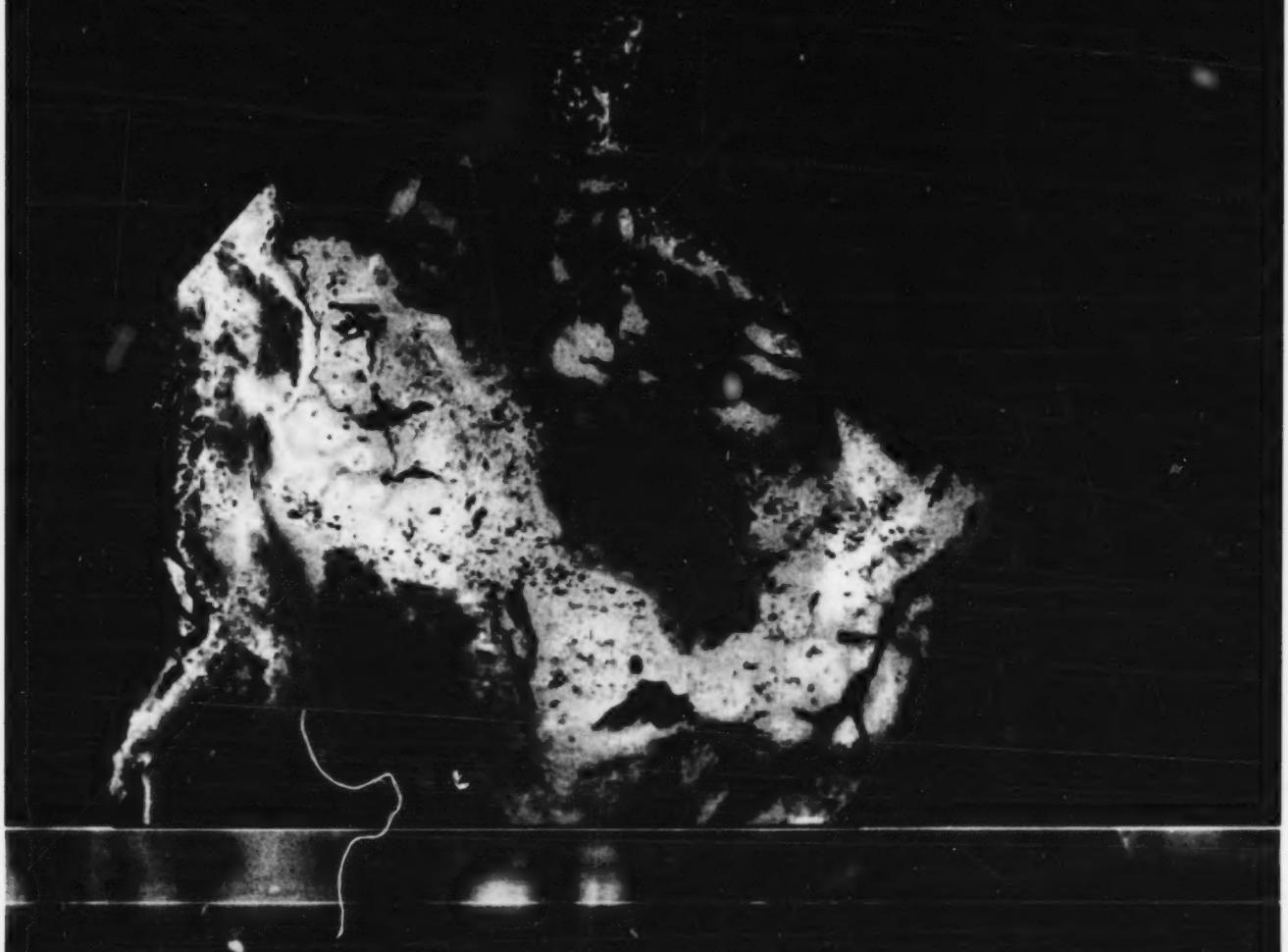
Biometrics:

Implications and Applications for Citizenship and Immigration



Report on a Forum hosted by
Citizenship and Immigration Canada

October 7 & 8, 2003 – Ottawa, Ontario

Public Policy Forum
Forum des politiques publiques

Biometrics:

Implications and Applications for Citizenship and Immigration

Report on a Forum hosted by Citizenship and Immigration Canada

October 7 & 8, 2003 - Ottawa, Ontario

Prepared by the Public Policy Forum for:

Citizenship and Immigration Canada

ABOUT THE PUBLIC POLICY FORUM

Striving for Excellence in Government

The Public Policy Forum is an independent, non-profit organisation aimed at improving the quality of government in Canada through better dialogue between the public, privacy and voluntary sectors. The Forum's members, drawn from businesses, federal and provincial governments, the voluntary sector and the labour movement, share a common belief that an efficient and effective public service is a key element in ensuring our quality of life and global competitive position.

Established in 1987, the Public Policy Forum has gained a reputation as a trusted, neutral facilitator, capable of bringing together a wide range of stakeholders in productive dialogue. Its research program provides a neutral base to inform collective decision-making. By promoting more information sharing and greater linkages between governments and other sectors, the Public Policy Forum ensures that Canada's future directions become more dynamic, co-ordinated and responsive to the challenges and opportunities that lie before us.

ABOUT THE AUTHORS

David Brown is Director, Special Projects, at the Public Policy Forum.

David Brook is an Associate of the Public Policy Forum

We would like to acknowledge the assistance of members of the Citizenship and Immigration Canada Task Force on Document Integrity, in particular Peggi McNeil, Director, and of Milena Isakovic, Research Assistant at the Public Policy Forum.

The Public Policy Forum
1405-130 Albert Street
Ottawa, ON K1P 5G4

Tel.: (613) 238-7160
Fax: (613) 238-7990

www.ppforum.ca

TABLE OF CONTENTS

INTRODUCTION 2

ANNEX I: SUMMARY OF INDIVIDUAL PRESENTATIONS 8

OPENING EVENT SPEECH: BALANCING SECURITY AND CIVIL LIBERTIES – Prof. Alan Dershowitz 8

OPENING REMARKS – The Honourable Denis Coderre 11

KEYNOTE SPEAKER: BIOMETRICS PAST, PRESENT AND FUTURE – Dr. Colin Soutar 13

PANEL SESSION 1: BIOMETRICS IN THE INTERNATIONAL CONTEXT 17

Martin Giles, Assistant Director, United Kingdom Immigration Services, Home Office 17

Gillian Russell, Directorate General, Justice and Home Affairs, European Commission 19

Dr. W. Russell Neuman, Senior Policy Advisor, White House Office of Science and Technology Policy 20

Gerry Van Kessel – Coordinator, Intergovernmental Consultations on Asylum, Refugee and Migration Policies in Europe, North America and Australia 21

LUNCHEON SPEAKER – Frank Graves 24

AFTERNOON SPEAKER: PRIVACY ISSUES – Stephanie Perrin 26

PANEL SESSION 2: BIOMETRICS - UNDERSTANDING AND ASSESSING THE IMPLICATIONS 30

Dr. Roger Gibbins, President and Chief Executive Officer of the Canada West Foundation 30

Jennifer Stoddart, Présidente, Commission d'accès à l'information du Québec 31

Raj Nanavati, International Biometrics Group 33

Raymonde Folco, Member of Parliament, Laval West 35

CONCLUSIONS AND DIRECTIONS FOR FUTURE ACTION – The Honourable Denis Coderre 37

ANNEX II: AGENDA 38

ANNEX III: REGISTERED PARTICIPANTS (AS OF OCTOBER 6, 2003) 40

ANNEX IV: TABLE DISCUSSION AND DIALOGUE 42

ANNEX V: SUMMARY OF PUBLIC POLICY FORUM BACKGROUND PAPER 44

ANNEX VI: SUMMARY OF INSTANT POLLING 46

INTRODUCTION

Recent international security concerns, border initiatives and the increasing incidence of identity theft and identity fraud have highlighted the need to strengthen the integrity of Canadian identity, immigration, citizenship and travel documents. Biometric technology has emerged as a powerful and controversial tool that could potentially help to address these public policy challenges. In this context, the Minister of Citizenship and Immigration of Canada, the Honourable Denis Coderre, has encouraged public debate on the issue of the development of a national identity policy and the possible use of biometric technology in identity documentation.

Over the past year, the House of Commons Standing Committee on Citizenship and Immigration has conducted hearings on the merits and challenges related to a possible national identity card. Following extensive consultations, it issued an interim report stating that this issue requires more in-depth study, including engagement with the Canadian public, before any definitive recommendations can be developed. This and related issues are also the subject of federal-provincial-territorial discussions.

On October 7 and 8, 2003, Citizenship and Immigration Canada (CIC), in an effort to advance the public debate, convened a Forum on Biometrics in Ottawa to look at the use of biometrics in the context of measures to enhance the integrity of identity and travel documentation for Canadian citizens and permanent residents (please see Annex II: Agenda).

The objectives of this Forum were to:

- Explore biometrics as a powerful technology that could meet important future policy objectives;
- Enhance and expand the existing discussion on technical and social issues related to the use of biometrics to strengthen document integrity and identity verification;
- Discuss comparative advantages and disadvantages of a comprehensive "national identity card" approach versus a more incremental strategy to improve current, multiple identity documents; and
- Engage in a dialogue on important issues prior to any policy implementation.

Structured around a combination of keynote speakers, panels, and group discussion and feedback, the Forum was designed to raise public awareness and to explore the possible implications and applications of the use of biometric technology in a citizenship and immigration context. The event engaged national stakeholders and international experts from interested sectors in a balanced dialogue to inform and advance the department's policy thinking on the substantive issues related to the use of biometric technologies to strengthen document integrity (please see Annex III: Registered participants).

In preparation for this event, the Public Policy Forum authored a Background Paper to inform CIC's policy thinking and to provide Forum participants and the Canadian public with a general overview of the key issues related to biometrics in the context of citizenship and immigration policy[1]. The paper was drafted at the request of CIC, on the basis of research and interviews with key experts (for a brief summary of the Background Paper, please see Annex V).

1 The Background Paper and other documents relating to the Biometrics Forum are available on a Web site created by CIC for the event: **http://cic-forum.ca/english**

In the course of the day-and-a-half session, participants and presenters initiated a dialogue on many of the issues identified in the Background Paper. This report seeks to present the key issues, challenges, directions and questions. It begins with an overview of the key issues that were raised during the Forum and in particular the common themes and points of consensus that emerged. The points made in each of the individual sessions are summarized in Annex I, along with questions and follow-up discussion with participants. In most cases, either the full text or outline notes are available on the Biometrics Forum Web site: **http://cic-forum.ca**.

At the end of the second day, the participants, who were seated at tables of six, were asked to have a "table discussion" on one of three questions relating to the use of biometrics and a possible national identity card. Each table was asked to record its views, and these are summarized in Annex IV. As well, on two occasions during the second day participants were asked to record their views and opinions using an electronic voting tool that allowed for an instant summary of the results. The results of these "instant polls" are summarized in Annex VI.

Forum Proceedings and Conclusions

The Citizenship and Immigration Forum on Biometrics featured a wide range of participants and presenters from many different backgrounds and jurisdictions (please see Annex III for a complete list of participants and presenters). Participants were selected to provide as wide a range as possible of perspectives, positions and opinions on identity, privacy and related issues. Given this diversity of participation, there was a lively debate and dialogue throughout the day and a half of the Forum on many key issues touching on the use of identity documents with biometric features in the citizenship and immigration context.

The Forum began with a keynote dinner address by Professor Alan Dershowitz, Felix Frankfurter Professor of Law at Harvard University (please see Annex I: pp. 8-11), who outlined some of the issues he perceived that relate to a national identity card and the use of biometrics. In his view, there are two key sets of issues: those pertaining to the card itself and those pertaining to its application. Professor Dershowitz emphasized the importance of having the debate about the use of biometrics now, so that policy can drive the development of technology, and not the other way around. He also argued that it is important not to rely on the failure of technology to protect privacy, but rather that issues such as privacy must be addressed at the inception of the development and implementation of any new technology, including an identity card with biometric features.

The morning session began with an introduction by the Honorable Denis Coderre, Minister of Citizenship and Immigration, who outlined the importance of the Forum and the urgency of dealing with issues of identity and the use of biometrics (Annex I: pp. 12-14). He suggested that, although there are a number of important issues to be addressed in relation to the use of biometrics, biometrics as a technology are here to stay. As such, in his view, the status quo is unacceptable and it is important for all Canadians to discuss and debate how best to improve document integrity in order to prevent identity fraud while still protecting the privacy rights of individuals.

The morning session continued with a keynote address by Dr. Colin Soutar, Chief Technology Advisor to the Canadian Advanced Technology Association Biometrics Group, and a leading expert on biometric technologies. He discussed some of the issues concerning the implementation of a biometrics-based identity card, such as the differences between verification and identification (Annex I: pp. 15-18). In his view, it is indeed possible to enhance security while also protecting identity, but this requires identifying the correct policy priorities and building technologies to meet these specifications.

The balance of the morning was spent with a panel of international representatives who discussed the role and application of biometric technologies in their respective contexts (for a complete list of the panelists, please see Annex II: Agenda. Notes on the panel presentation are in Annex I: pp. 19-27.) Panelists discussed the role of biometric systems in immigration in the European Union, through the use of the EURODAC system, and in the United Kingdom. They also examined the importance of biometric technologies to the security agenda in the United States, and the potential use of biometric technologies in the context of immigration and refugee movements to Canada.

During the question period which followed the international panel, participants expressed concern over the potential to create a "we-versus-them" mentality by imposing biometrics in an immigration context. Panelists responded that legitimate users of the immigration system are generally in favour of a single card with a high level of integrity that allows them to access the services they need with a minimum of difficulty. Other Forum participants expressed concern about the potential for abuse of a biometric system. The panelists responded by stating that any system is open to abuse if approached in an inappropriate or irresponsible manner. As such, it is important to ensure an open and transparent debate on the use of biometrics in any given application.

The luncheon speaker was Frank Graves, president of EKOS Research Associates Inc., who presented recent quantitative data on the views of Canadians (Annex I: pp. 28-30). Mr. Graves argued that a clear majority of Canadians would be willing to support the implementation of a national identity card, were they given a compelling reason to do so, but that Canadians do not see the need to trade off security against privacy. He stated that Canadians will demand a high level of both and are not willing to compromise on either.

The afternoon session began with a presentation by Stephanie Perrin of Digital Discretion, who outlined some of the privacy concerns relating to the use of biometrics and the implementation of a national identity card (Annex I: pp. 31-33). Ms. Perrin raised questions about the need for biometric solutions to identity-related issues and stressed the importance of independent oversight of biometric applications and the need for more research into the longer-term implications of the implementation of any national identity card.

The afternoon panel focused on understanding and assessing the privacy implications of biometric technologies in a Canadian context (for a complete list of panelists, please see Annex II: Agenda. Notes on the panel presentation and subsequent discussion are in Annex I: pp. 34-42.) The panelists raised a number of questions regarding the purpose, uses and nature of a national identity card. They also examined the importance of privacy legislation, independent oversight of the use of biometric systems and of data collected through them, and the need to look at alternatives such as improving the integrity of other "root" or "foundation" documents (such as birth certificates). Finally, one of the panelists advanced an argument in favour of a principles-based approach to the use of biometrics.

During the discussion that followed, participants and panelists emphasized the need to ensure the appropriate deployment of biometric technologies, the importance of independent oversight and auditing, and the need for the government to make a compelling case before pursuing the implementation of a national identity card.

The session concluded with participants discussing, at their tables, three issues relating to biometrics, followed by brief reports to the plenary group. The points raised in these deliberations are summarized in Annex IV. Minister Coderre closed the Forum with brief remarks emphasizing once again his belief that biometric technologies are here to stay and that this issue is vital to all Canadians (Annex I: pg. 43). He

expressed his desire to inform Canadians about this issue and to encourage discussions in living rooms across the nation.

Although a consensus did not emerge over the course of the session, nonetheless there were a number of areas of commonality and agreement in support of an agenda to move forward. These key issues, concerns and areas of agreement were:

The use of biometrics in identity documentation presents genuine issues that merit serious public discussion.

- The issues relating to identity documentation have a direct impact on all Canadians. At the same time, public awareness of these issues and of the choices they represent is low and tends to be impressionistic.
- There is currently a policy and legislative vacuum in a rapidly evolving area of public policy.
- Canada has considerable expertise that is relevant to this discussion, both on the technology side and in closely related areas such as privacy and data management. International experience is also relevant, both in providing best practices and because of the interdependent nature of areas of public policy such as immigration.
- There is considerable common ground among knowledgeable experts, recognizing that this is an area that requires a multidisciplinary and multi-jurisdictional approach.

The status quo is not sustainable.

- Canadians cannot rely on the failure or incompetent use of technology to protect their privacy.
- Biometric technologies are now being applied and their use will only grow. It is therefore important to engage in a full and open public debate with respect to their purpose, use, and necessary safeguards against potential abuse.
- It is important to make sure that policy imperatives are driving the development of technology and not technology driving policy.

The perceived dichotomy between security and privacy is false.

- By the end of the Forum, many if not most participants and presenters agreed that although there may be challenges with the use of biometrics in some contexts, there is nothing either inherently privacy-enhancing or privacy-limiting about the use of biometrics. Biometrics must therefore be looked at in the context of specific applications and their related data management environment.

There needs to be a business case for using biometric applications in identity documentation, including a national identity card.

- Participants agreed that there is a real need to define the issues that would be addressed by using biometric tools in identity documentation and the public policy challenges that a single national identity card with biometric features would help to meet.
- These definitions would would make it possible to identify more fully the functions, purposes, uses and safeguards that would be necessary to implement such a card.
- Only when this crucial policy work is completed could a comparison be made between the costs and benefits of a national identity card and other document integrity solutions.

- An important preoccupation for many participants was the cost of establishing a national identity card, including the implementation of an effective process for registration and administrative mechanisms that would be necessary to make it functional on a day-to-day basis. Although there was no agreement on the potential costs of such an endeavour (with estimates ranging from Cdn $340 million to more than Cdn $5 billion), there was general agreement that before such a card can be considered it is absolutely vital to undertake a thorough cost/benefit analysis.

Biometrics have been successfully applied for specific uses in other jurisdictions.

- Presentations throughout the day indicated that biometric identifiers have been successfully used in jurisdictions outside Canada, in the context of addressing clearly identified needs, such as those relating to immigration.
- Some of the lessons from the international examples include:
    - o The importance of developing and implementing programs using biometric tools on the basis of sound policy and good management.
    - o The importance of understanding the particular application or applications in which biometrics will be used.
    - o Privacy safeguards must be built into the system from the outset if they are to be effective.
    - o There is a need for effective independent oversight of any technology system that presents a danger of compromising the privacy of any individual or group of individuals.

There are a number of technical issues that would have to be addressed before a biometrics-enabled national identity card could be implemented.

- Participants identified a number of technical challenges and considerations that would need to be considered in the development and implementation of a biometric card, including:
    - o Whether the core use of a card is verification or authentication.
    - o Ensuring accuracy in the operation of the biometric features and related data management.
    - o The method of capturing and processing biometric information (use of an image versus a template).
    - o The type of biometric to be used in light of the very different balance of considerations that applies in each case.

A national identity card, if introduced, should be mandatory and not voluntary in nature.

Arguments were presented in favour of both a voluntary and a mandatory approach, however over the course of the Forum the balance favoured making any possible implementation of a national identity card mandatory in nature. Such arguments included:

- o The danger of excluding groups who may not be able to access or afford a voluntary card.
- o The need to make sure that any infringement on civil liberties is distributed across the entire population, ensuring an open and balanced policy debate.
- o At the same time, several participants cautioned against the risk of "function creep" in any national or universal card.

Privacy and data protection issues must be satisfactorily addressed as an integral part of designing and implementing any identity documentation using biometrics.

- Participants expressed concern over a number of potential privacy issues:
    - Unauthorized access to information – participants had a number of concerns around the availability of information that was collected using biometric tools, either to unauthorized government agencies and agents, or to the private sector. A closely related issue is whether and under what terms data would be re-used or shared with others.
    - Function creep – many participants expressed the belief that any card, despite its initial purposes for implementation, will expand in terms of the functions for which it is used. There was particular concern about the extension of a government-issued card's functions into the realms of providing access to government services or even commercial transactions (as is happening in a number of other countries).
    - Privacy principles – at the same time, it was agreed that internationally and nationally accepted privacy and data management principles offer a sound basis to work from in order to regulate the use of biometrics and that useful legislative models exist in Canada.

In the end, participants agreed that there is a need for a "made in Canada" solution to the issue of identity documentation. At the same time, it was recognized that international pressure to implement some form of biometric application, whether restricted to travel documentation or broader in nature, will only increase in the coming years. As such, it would seem that there is a clear and compelling case for the federal government to develop and implement a policy and strategy on identity documentation issues, including the use of biometrics, within its own jurisdiction and to work with the provinces and territories in developing a national approach to these issues. It should also continue to work with international discussion of these issues.

ANNEX I: SUMMARY OF INDIVIDUAL PRESENTATIONS

Opening Event Speech: Balancing Security and Civil Liberties – Prof. Alan Dershowitz
Felix Frankfurter Professor of Law
Harvard Law School

Professor Dershowitz began his speech by deconstructing the issue of the development and implementation of a national identity card into two sets of issues:

- those relating to a national identity card itself, and
- those related to its application in a particular setting.

The first set of issues (those relating to the card itself) are:

1) What type of card to use?

- Would it be a minimal card that might include an individual's name and citizenship, or a maximal card that might include every piece of identifying information about an individual, including their criminal record? Would the card include a biometric identifier?

2) When should government be empowered to require identification?

- When should citizens be able to refuse to identify themselves? It could definitely be argued that the 'feeling of freedom' would be lost if a police officer could ask an individual to produce their papers at any time, for any reason. On the other hand the 'feeling of security' might be compromised if an individual could never be compelled to produce identification.

3) How can you guarantee that the information on a card matches the holder?

- For Professor Dershowitz, this represents two issues: whether an individual presenting a card is the individual represented on the card, and whether the person on the card actually is who they say they are. In his view, the former issue, in particular, lends itself to clarification through the use of a biometric identifier. The latter points to the need for good background checks.

4) Should the card be mandatory or voluntary?

- Professor Dershowitz outlined a number of questions concerning the mandatory versus voluntary implementation of a national identity card. To introduce this discussion, he gave the example of a 'trusted fliers' program that allows one to move through an airport line more quickly if specific criteria are met. The proof of enrollment in such a program could be based on a biometric identifier. Professor Dershowitz asserted that such an application would probably be acceptable to the majority of individuals if the only consequence of non-enrollment was that the non-enrolled individual would be forced to wait in a somewhat longer line. If, however, the enrolled individual moved through the line in minutes, while the non-enrolled individual faced a multi-hour wait, how voluntary is the choice to enroll? Other related questions, in Professor Dershowitz's opinion include:
    - If a card were mandatory, would everyone have to carry it all times?

- If not, would an individual have a grace period within which to produce the card when properly requested to do so?

5) Should an identity card be local, national or international in scope?

- Professor Dershowitz stated that there are advantages and disadvantages to each of these scenarios, but that currently, international standards (such as for driver's licenses) are not widely in use. He mentioned that in the United States efforts have been made to institute a national driver's license, but some conservative as well as civil liberties groups oppose such a plan, with strong opposition even to the institution of a standard-format license across all states.

The second group of issues identified by Professor Dershowitz were those concerning the specific application of a national identity card in a real-world setting, including:

1) What kind of database would be connected to the card?

- For Professor Dershowitz, important questions in this regard include:
  - What information should the database contain?
  - Would it be linked to a single or to multiple databases?
  - Would there be information-sharing between different databases?

2) Should the private sector be able to access this information?

- Professor Dershowitz indicated that there need not be a difficulty in accessing various databases from a single card, as long as the firewall between the databases is sufficiently secure.

3) Is it possible to limit the accessing of information on a national identity card to a 'need to know' basis only?

- Technically, Professor Dershowitz asserted, it is possible to limit access to information. He offered the example of the Malaysian identity card which, as of a few months ago, contained much more information, in his opinion, than any Canadian or American citizen would permit their government to collect in any one place. He indicated that the key to the acceptance of the Malaysian card, however, has been the assurance that no one government agency can access all the information that is contained on the card, as this information is segregated by firewalls and is available on a "need to know" basis only.

Professor Dershowitz continued his address by stating that it is important to have a debate about what kinds of technology are appropriate and in what situations well before the technology is available and on the market, so that policy considerations drive the development of technology and not the other way around. He reinforced this point by stating that one cannot be insensitive to the abuses that can arise from the centralization of power. It is also important to debate what kinds of information are appropriate for governments to gather and hold in databases.

From his general discussion of issues relating to a national identity card, Professor Dershowitz moved to a more in-depth discussion of the ways in which such a card might be implemented. In his view, there are many ways that a national identity card could function – when an individual puts it in a machine, it could give a negative or positive identification, or it could feed out enormous amounts of information from a central database. Either of these functions could be used in any number of applications. He then addressed the concern among some privacy advocates and other participants about the potential for a 'slippery slope,' meaning that the use of ID cards could expand from their primary intended functions to include

other unintended functions that are more invasive of privacy. He stated that the only thing more dangerous than a slippery slope is an 'invisible slippery slope,' recognizing that any card, biometric or otherwise, that offers an improvement on existing methods of verifying identity will undoubtedly begin to be used for unrelated functions. As such, he contended that it is better to have an open and public debate about the possible uses for such a device, rather than letting it be adapted to other functions without debate or scrutiny.

One argument which Professor Dershowitz presented in favor of the implementation of a minimal national identity card was that it could limit the need or rationale for ethnic or national profiling. He argued that if a country is going to diminish rights, it is better for it to spread the diminution of rights across the entire population than to focus it on minority populations (such as American Muslims, following the attacks on September 11, 2001). He stated that if the diminution of freedom is spread across the entire population then there will be a balanced and equitable distribution of any resulting hardship and, as such, there will much more likely be a full and lively debate about its impacts on the population.

Professor Dershowitz then raised the example of the use of face-recognition machines in public places. He argued that although these machines do not currently work well enough to be implemented (they produce far too many false positives and failures to recognize to be effective), they will reach acceptable standards at some point in the near future. He stated that society must start debating the issue of the use of these technologies now, because otherwise it will be too late to initiate a dialogue on these issues when the technology is developed and in place.

One of the central themes of Professor Dershowitz's presentation was the proposition that it is a major error to depend on the inefficiency of technology to protect privacy. He argued that this is a mistake because all technologies, even those which currently seem extremely fallible or remote in their development, will eventually work well enough to be implemented. Therefore, the ideal is to create a "win-win" technology, one that enhances both privacy and security. He stated that policy-makers need to tell the machine-makers what kind of technologies they need to design and create, and that policy-makers need to find ways to increase both security and liberty.

Professor Dershowitz followed his presentation by answering a number of questions from Forum participants. Several participants picked up on his theme of the dangers of function creep (the slippery slope), and expressed concern that this would be an inevitable danger associated with the implementation of any national identification card. In response, he stated that the whole point of having a full and open debate around these issues is to ensure that function creep is not allowed, or at worst, that it occurs after a full and open debate. In his view, doing things in the open is always going to be better than doing things under the table. As such, his final advice to participants was that whatever Canada does in relation to the issue of a national identity card, it should do it openly. He stated that it is important not to count on 'good' coming from the status quo, but to use technology to help solve problems and protect the public good. By the same token, it is important not to reject technology in the belief that good things will flow from inefficiencies.

Opening Remarks – The Honourable Denis Coderre Minister of Citizenship and Immigration Canada

Minister Coderre opened the session by stating that the debate over identity documentation and the use of biometrics is very important to the lives of Canadians[2]. He indicated that, despite differences in perspective among the Forum participants, some issues are universal in scope and must be the subject of a healthy dialogue to allow the country to move ahead. The "biometrics train has left the station," and the issue needs to be discussed with an open mind.

Mr. Coderre identified some of the key issues that Canada must address in the near term, including how to improve document integrity, protect against terrorism and identity theft, and meet emerging international requirements. Document integrity is an issue that all countries face and measures are being taken by the United States, the International Civil Aviation Organization and by the G-8. The question, therefore, is whether we as Canadians want a "made in Canada" solution to these challenges, or one that is imposed from the outside. The planet is getting smaller and documents are increasingly important in the face of the realities of security and terrorism.

A closely related question for the Minister was whether Canada can both protect and enhance privacy while also improving security and ensuring identity. He stated that it seems very clear that this is indeed possible. The entire issue of document integrity is becoming more important since Canadians expect their government to be able to ensure that the people who come to Canada are who they say they are. Canadians also expect the documents they use to access services to be resistant to tampering and fraud and to maintain their integrity over time.

A card is not the full answer to these issues – it fits in a larger set of measures including notably a response to identity theft and identity fraud, which cost Canadians $2.5 billion a year, according to the Canadian Council of Better Business Bureaus. In the United States, the Federal Trade Commission estimates that 10 million Americans were victimized by these crimes in the past year. Statistics show that a thousand people a month report crimes of identity theft to the police, with many more cases unreported. So, while the program cost of a national identity card might be high, the cost of not acting to protect citizens and the economy would be high as well.

Minister Coderre stated that the government understands the need to act. Citizenship and Immigration Canada is in the process of issuing two million new Permanent Resident Cards, a program which has been well received. The use of biometrics is becoming wider spread, and several provinces are considering their introduction, including some that are thinking of using retinal scans and fingerprints on driver's licenses. There is a growing lobby in the United States that wishes to see the implementation of a standardized license with biometric features in every state. Measures are also being taken in the context of airport security. Action on the privacy side is also important, and Minister Coderre flagged the implementation of the new *Personal Information Protection and Electronic Documents Act*.

Minister Coderre stated that the federal government is adopting a more integrated approach to these issues, with Citizenship and Immigration Canada taking a lead on document integrity matters. Doing nothing and hoping for the best is not an option. He outlined two broad possible approaches to improving document integrity:

2 A complete transcript of the Minister's speech is available on the Citizenship and Immigration Biometrics Forum Web site: **http://cic-forum.ca/english**

- A new comprehensive national approach, including looking at options such as a national identity card, or
- An incremental improvement of existing foundation documents.

In either case, in his view, it will be important to look at developing a card (or cards) that make the most of available technologies and that apply best practices. A comprehensive approach might be along the lines of national identity documents adopted by more than 100 countries. The House of Commons Standing Committee on Citizenship and Immigration is already examining these approaches and has studied all aspects of the issue. Fundamentally, the Standing Committee members are asking if a comprehensive approach to the issue of identity is better than an incremental process – can it be used to replace the range of cards now in use by Canadians?

Minister Coderre continued by asserting that, as a country, Canada can also choose to take an incremental approach to improving document integrity that focuses on improving the documents that we already have – and biometrics can be part of this process. He felt it important to note, however, that Canadians already have many kinds of cards that provide information to the government, so it is important not to confuse a desire for anonymity (which Canadians do not currently possess) with the desire to protect an individual's privacy. He suggested that Canadians have already witnessed changes to documents such as their driver's licenses, which are now made of plastic and have photos embedded in their design, and that such changes will only become more commonplace. The names of Canadians appear in many databases and a wide array of individuals and organizations have a considerable store of personal data on many Canadian citizens. In responding to this situation, Canada has two fundamental options: it can maintain the status quo with respect to the privacy of individuals in Canada, or it can look at all the available options to strike a new balance that both enhances security and protects privacy.

In relation to the issue of the identification of landed immigrants in Canada, Minister Coderre stated that the new Permanent Resident card is a better and more secure card than its predecessor document. In his view, however, there is potential to enhance the security of this card through the use of biometric identifiers, which it is capable of incorporating. This leads to some important questions that remain to be addressed:

How do we meet our need for a higher level of security in identity documents?

How do we protect privacy and address concerns about the erosion of our civil liberties?

What would a national identity card cost?

Do we have a cost/benefit analysis that can accurately predict the costs and savings to Canadians?

With respect to the latter point, the Minister suggested that it is important first to agree on concepts and then to discuss costs; the first question that needs to be asked is whether Canadians want a national identity card? This question could be framed by asking what future documentation should look like and how it should be authenticated. In his view, if Canadians were to decide that a national identity card might potentially be a useful tool, then the government should do a cost-benefit analysis and make a business case for its implementation. He stated that the Permanent Resident Card will be issued to approximately two million Canadians and will have an estimated net cost of $22.9 million to implement.

Minister Coderre stated that Canada needs an informed debate on the implementation of a national identity card and that the government needs to put the facts and issues on the table. A decision needs to be made based on sound public policy that will lead to real, tangible improvements for Canadians. Finally,

he asked the rhetorical question, why is Citizenship and Immigration Canada hosting this conference? He responded by stating that, firstly, the department has a duty to explore the implications of any new technologies that could have an impact on its mandate and that would allow it to do its work better. Secondly, Canada needs to look beyond its borders, at other countries such as the United States, the United Kingdom, the European Union, Australia and New Zealand, both to learn from their experience and to look at the impact of what they are doing on Canada.

Canadians have to move beyond thinking about the technical issues involved in implementing a national identity card to thinking about the public policy issues that it would address, and whether these issues present a compelling case for its implementation. The best tools combined with poor policy will simply condemn us to failure, and any use of biometrics as a form of identification and verification must be done in such a way that protects privacy and freedom and that is transparent and open to Canadians in order to ensure accuracy and to prevent abuse.

Canada has a solid basis, however, for developing its policy choices. The *Charter of Rights and Freedoms* and our judicial system give us a base to ensure that we will not become a police state. We can develop a legal framework for the use of biometrics in identity documentation. Biometrics are coming – the Europeans are moving beyond identity cards to smart cards providing access to government services. This is an issue that touches on all aspects of daily life and that requires inclusive solutions.

In concluding, Minister Coderre stated that the discussion in the Forum on Biometrics will be used to develop policy options for the government and to help him as he speaks to his ministerial colleagues and to his international counterparts. This is one of the most important debates of the next decade. The government has a duty to ensure an inclusive, serious debate to allow Canada to adapt to the 21st century.

Keynote Speaker: Biometrics Past, Present and Future – Dr. Colin Soutar
Chief Technology Advisor
Canadian Advanced Technology Association – Biometrics Group
Chief Technology Officer, Bioscrypt Inc.

Dr. Soutar began his presentation by stating that the issue of the use of biometrics in the context of a national identity card is a controversial subject. As such, he made the decision to focus his talk on some of the issues around the use of biometrics in conjunction with the development and implementation of an identity card, and to discuss some of the standardisation efforts that are underway with respect to biometrics both in Canada and internationally.

Within this context, Dr. Soutar indicated that there are a few crucial considerations that must be evaluated in deciding the appropriate implementation of biometrics for a given application. Indeed, he asserted that there are two or three subtle points that are very important to understand in terms of the impact of biometrics on a system as a whole and which have a profound impact on the appropriate deployment of biometric technologies.

As a reference point, Dr. Soutar reviewed some of the current international initiatives with respect to biometric standards. He indicated that the International Standards Organization (ISO) as an organisation is keenly interested in the use of biometrics and that it has a committee, which is currently in the process of defining international biometric standards. He indicated that Canada is a forerunner in the evaluation of security devices and that Canadians (including himself) are helping to define what will, in the future, become international standards.

Dr. Soutar identified four features - fingerprints, iris, hand and face geometry - as being currently the most popular biometric features, from the point of view of international standards development and commercial deployments. He clarified that it is important, especially from the perspective of public perception, that biometrics do not identify a person, but rather that they recognise that someone has been enrolled in a system previously - based on either a search of a database or a one-to-one match. He stated that biometrics could not pick someone out of a crowd, if they have not been previously enrolled, but they can tie a system identifier to an individual.

He asserted that in an appropriately defined system, biometrics could provide additional security and protect confidentiality at the same time. In his view, it is a public policy issue to define the acceptable balance between the protection of civil liberties and the enhancement of security that will be captured within a system. One example he offered of different types of technologies having a differential impact on privacy was the difference between technologies that provide verification and those that identify individuals.

At its most basic, the process of identification uses a database to determine who an individual is, while off-line verification simply demonstrates that an individual matches an identifier on a card. Dr. Soutar stated that it is possible to store information for verification locally (on a card) while identification must take place centrally with the use of a database. In his view, a key challenge with any system of identification is the need for a simple and efficient way to revoke rights and privileges of card holders.

Dr. Soutar argued that the use of biometrics should be complemented with cryptography and smart cards to provide optimal implementation. In other words, technologies need to be combined in order to create an effective system. He also stated that a much broader range of biometrics is currently being deployed than previously and that these technologies are now being combined in novel ways. Some of these novel uses include:

Positive identification - which is useful anywhere where a password or pin is currently used, for example: long distance calling cards, banking, entry to buildings, etc.

Access control - Dr. Soutar used the example of American Express, which uses a smart card with biometrics at their headquarters for purposes of worker verification (to accurately verify who is doing what in the building at what times). This card is local and is used to access buildings across multiple facilities. The New York Police Department also makes use of this technology.

Timekeeping - Another application for biometric cards, which Dr. Soutar described, is time and attendance. He explained that if a number of employees have access to a safe with a biometric system, any individual employee in the presence of the safe at a given time could be accurately identified.

Dr. Soutar concluded this section of his presentation by stating that biometrics are not "coming in the future;" in his view, they are here today.

The next issue, which Dr. Soutar addressed, was the choice of verification versus identification for a biometric system. He indicated that identification can be used for functions such as background checks and involves access to a central database, whereas verification can be used on a daily basis to verify that someone is the valid holder of a card, a process involving only a local data set. As such, he argued, the mathematical matching algorithms for these two operations need not be the same, even though a single acquisition of the biometric can be used for both purposes.

As an example of the uses of verification to protect privacy, Dr. Soutar stated that a user could establish a unique identity via documents such as a birth certificate. A system identifier such as a passport number could be bound to the user's verification template[3] to create a record. In this scenario, the identifier is used only to confirm that the individual who presents the card is who they state they are, and the biometric data is not linked to any other information. Dr. Soutar repeated the point that biometrics themselves do not identify individuals; rather, they recognise that individuals are legitimately enrolled in a system.

Dr. Soutar indicated that a system based on biometric verification would allow for the seamless integration of the new biometric technology with an existing non-biometric system. In this scenario, the 'internal guts' of the database system do not need to know that a biometric is being used to verify the identity of a card holder; the database system is still tied to a separate identifier such as a passport number. Such a system allows the application, not the biometric, to control the rights and privileges of the individual. It also allows the application to easily revoke these rights if necessary.

In Dr. Soutar's view, using an identifier and a verification template also avoids the problem of profiling[4] – all the system needs to know is that a valid passport number is being entered, not who is holding the passport. Once the system has verified the identity of the card holder and shown his or her validity, then the associated passport number is sent to a central application that indicates whether a passport number is valid or not. The implementation of such a system would mean that an officer never has to make the decision about whether someone may validly enter a country; this can be done centrally.

So, can such a system be implemented within Canadian privacy legislation? Dr. Soutar argued that Canada has a good set of privacy standards. Individuals will have expressed their consent when they enrol in a program – they will have an awareness of why the template of their information is being created. He indicated that two privacy principles are of particular importance in this case: the confidentiality of user and of biometric information. In his view, it is important to safeguard the user record by using encryption technology so that the data block cannot be tampered with. He stated that this information can be stored on a bar code and is a very important contributor to the system's integrity.

Dr. Soutar argued that such a system could prevent identity theft and hinder the ability of individuals to use false identities in the commission of terrorist acts. Also, in his view, the separation of user verification from system authorisation limits the danger of function creep.

Dr. Soutar concluded his presentation by discussing the possible uses for biometrics in the future. Some of these uses will involve the fusion of biometrics for convenience and security, such as the combination of face and finger systems and multi-algorithm methods. Another important development, in his opinion, will be the implementation of key binding algorithms, such as templates that are application-specific. A further development might be the use of smart tokens for multiple applications. For example, a key fob could become a multiple key repository, which could access an individual's computer, finances or personal device and would allow the sharing of specific personal information for various purposes.

During the discussion that followed his presentation, a concern was raised that the coding used on cards (for instance the number on a passport) could provide clues as to the identity of the bearer. Dr. Soutar indicated that, in effect, there is no limitation on the identifier, as it does not even have to take the form of a code. He stated that if it makes more sense to have a pseudo-random number assigned as an identifier,

3 A verification template is a unique set of information related to a biometric identifier (such as a fingerprint), which is recorded on a device such as a card, against which a new acquisition of data can be tested.

4 When an agent or officer singles out an individual or group of individuals for particular attention based on an identifier such as race.

then that could be the case. As well, he argued, the number never has to visually appear on the card as it could be encrypted for added security. Finally, he indicated that, from his perspective, any system could potentially be abused, so an analysis of the potential for abuse will have to take place alongside the policy debate surrounding these issues more generally.

Another participant asked whether the use of identification technologies could be used to reduce the incidence of acts of terrorism. Specifically, they asked whether positive identification could stop a rogue officer from doing something untoward, even in an environment that used biometric identification technologies. Dr. Soutar replied by stating that these technologies can enhance security in several different ways: they can act as a deterrent; they can help to prevent identity theft; and, finally, enrolees can be asked to go through a screening process such as that involved in becoming a Canadian citizen – such a screening process can be tied to the ability and capacity to revoke privileges very quickly, if necessary.

Panel Session 1: Biometrics in the International Context

Martin Giles, Assistant Director, United Kingdom Immigration Services, Home Office

Gillian Russell, Directorate General, Justice and Home Affairs, European Commission

Dr. W. Russell Neuman, Senior Policy Advisor, White House Office of Science and Technology Policy

Gerry Van Kessel – Coordinator, Intergovernmental Consultations on Asylum, Refugee and Migration Policies in Europe, North America and Australia

The purpose of the morning panel was to provide an overview of how biometrics are being applied in the international context. The first three panelists were invited to describe the experience in their respective jurisdictions (United Kingdom, European Union and United States), while the fourth panelist was a Canadian working in the intergovernmental environment on immigration and refugee issues.

Martin Giles
Assistant Director
United Kingdom Immigration Services, Home Office

Mr. Giles began his presentation by stating that terrorism is an international problem and requires international cooperation. He continued by describing his involvement with the development and implementation of an immigration biometric identification program in the UK For Mr. Giles, the issue of establishing identity in the immigration process is complex, traditionally relying on passports as a way to identify individuals, provide names, date of birth, nationality and some indication of prior travel. He indicated, however, that this system has begun to break down as many of the individuals who have come to the UK in recent years have destroyed their documents for a variety of reasons.

The very concept of identity itself is interesting, for Mr. Giles, in that most people identify themselves in terms of their names and the area where they live, and yet these things are not unique and thus cannot form the basis of an accurate identification. In his view, biometrics can show the uniqueness of a human being, but only if that individual has not been previously enrolled in the system. The aim of the immigration identity program, therefore, is to ensure that any individual has one, and only one, identity for the purposes of the program.

Mr. Giles stated that in 1999 the UK had a manual system of collecting fingerprints from asylum applicants, a system that was very slow and similar in nature to that in use by Scotland Yard (i.e., by the police). It was taking six months for a fingerprint check to be verified, which was deemed to be an unacceptable length of time. The decision was therefore taken in the late 1990s to re-build the system. As part of their discussions, policy-makers considered whether they should continue to use fingerprints as an identifier or whether they should adopt a new standard. Mr. Giles stated that, for a number of reasons, the decision was made to stay with a fingerprint record: fingerprints are unique, the AFIS (Automated Fingerprint Identification System) is a tried and tested methodology, there are existing records and a statutory right to exchange data with others, in particular the police, and staff were already trained to take fingerprints, which are accepted as evidence.

The original objective of the program to automate the collection of fingerprints from asylum seekers, as outlined by Mr. Giles, was to allow fingerprint tests to be conducted anywhere and to have the results of

these checks available in less than an hour. These parameters were based on the operational experience of the project managers. As a result, currently in each asylum screening unit there are five scanning units and card scanners that can scan in ink fingerprints; these are linked to quick-check units that rely on GSM technology (a second generation wireless technology) and use cell phones to connect to the central system. Mr. Giles stated that the original test project has since been developed into a full program from which biometric cards have been issued that are connected to EURODAC (a European Union-wide database for tracking asylum requests, discussed in the next section of this report). The test project has also led to a similar project with direct links to the police system and the use of this data in visa applications. Finally, Mr. Giles indicated that the system cards have been used to close a loophole that existed in the immigration system whereby individual asylum seekers could change their names and register multiple times in the system.

In Mr. Giles' view, the program has been very successful – multiple applications have been reduced from six to one per cent of the total number of applicants, quick checks are regularly identifying murderers, rapists and other criminals as they access the system, and the application reporting cards are decreasing National Asylum Support Services payments and deterring people from applying for these services by proxy. EURODAC has also identified over 1100 third party applicants, and a recent trial has shown that almost 60 per cent of multiple applicants are being detected by the system.

Mr. Giles stated that there has been vigorous debate around the choice of biometrics for use in this program on an ongoing basis. At the same time, however, in his opinion the benefits are real and tangible. He indicated that some other policy areas where the use of biometrics is being considered include:

- The prevention of the creation of multiple identities,
- Benefit fraud reduction,
- Reporting management,
- Biometric visas,
- Fast-track security clearance,
- Internal security with the Immigration Services (access control and anti-corruption), and
- Biometric passports.

Mr. Giles concluded his presentation by outlining some of the lessons learned from the program. These include:

- Less than 100 per cent accuracy in detection is acceptable as the system can still catch almost 90 per cent of the cases.
- The production of ID cards is difficult when it is dispersed throughout a jurisdiction, but these technical challenges can be overcome.
- Real savings can be realized through the appropriate use of a biometric card system, but biometrics are a new technology and there is considerable ignorance about their use and implications.
- There is a need for international biometrics standards to be able to work in a multi-jurisdictional context. No matter how strong a documentary system, it simply cannot compare with iris and fingerprint-based identifiers.
- Finally, good administration and management are keys to success.

Gillian Russell
Directorate General, Justice and Home Affairs
European Commission

The primary focus of Ms. Russell's presentation was the EURODAC system, which is currently in use in the European Union to keep track of asylum applications in the European Union. Specifically, she focused on some of the issues relating to its successful implementation, and then went on to discuss some new applications for which the EU is considering the use of a biometric database.

Ms. Russell began her presentation by emphasizing the importance of public policy in creating a system such as EURODAC. To this end, she indicated that EURODAC was created as a legal entity only after 10 years of debate about the best way to address the challenge of how to quickly determine if people have applied for asylum in more than one member state. Due to a legal situation, Denmark is excluded, but the system also includes Norway and Iceland (making 16 Member States), and the Swiss are currently negotiating their participation. She stated that EURODAC is the first European-wide biometric database that allows different countries to use their own proprietary information. In fact, each country can use its own system to store fingerprint and other information on the applicant (such as name and sex), but only fingerprint data is transferred to EURODAC for the identification process.

Ms. Russell stated that there are three categories of data in use in EURODAC:

> **Category 1** – asylum seekers over 14, for whom data are stored for 10 years,
>
> **Category 2** – cases of apprehension in an irregular crossing of an external border of the EU, which is stored for 2 years, and
>
> **Category 3** – individuals who are illegally present within a member state, to check for asylum status.

Identification in category 3 could be done with a two finger check, although this is not normal, while other categories require a full 10 prints. Member states are responsible for the gathering and collection of data at one point (national access point), which then sends it to the Central Unit. She indicated that data for the EURODAC system are transferred on the European-wide IPVPN, an Internet-like network that is fully encrypted. Further, she stated that it takes less than five minutes to respond to queries. The system was launched in January 2003 and will expand to include another 10 countries in 2004. It can only be down for 40 minutes per 28 days, which is a very demanding requirement for level of service.

Ms. Russell also gave an overview of some of the different applications in which the EU is considering using similar technologies, such as the system that is used to apply for entry visas to the Schengen group of member states. The common problem to be addressed in this system is that the verification and identification of individuals who have applied for an entry visa in more than one state is an extremely complex task. She indicated that there are some interesting technical challenges to be overcome before such an application could be implemented, with biometrics hopefully providing a useful answer. Indeed, there is a proposal on the table to use biometrics (facial and fingerprints) in new entry visas that would be used solely for identification purposes.

Finally, Ms. Russell discussed some of her concerns about the robustness of some of the new technologies that are currently being proposed, indicating that she is not sure if there has been sufficient research into their effectiveness for very large applications. She stated that there is a strong need for some form of harmonization and that systems will not be able to inter-operate if there is not a common standard in use globally.

In the future, the interchange of data between jurisdictions will depend on standards; this issue is being looked at in many fora including G-8 and other interested international bodies.

To conclude, Ms. Russell stated that in implementing such systems, it is important to be very careful about privacy, an issue which is currently managed by independent bodies in Europe within a legal framework. With EURODAC, the data that is stored belongs to the member state that sends the information. She asserted that these independent bodies can look at how logging is undertaken for the entry and retrieval of data, and how long the logs are kept and provide a means by which anyone can check if their data is stored legally. Within the scope of the other applications the EU is considering, the EU is conducting a considerable amount of research to try to ensure that the technologies that are developed and implemented aid in the development and implementation of good policy to balance the rights of the traveler against various technical and operational objectives, and that there is a coherent approach to the problem of identification.

Dr. W. Russell Neuman
Senior Policy Advisor
White House Office of Science and Technology Policy

The central focus of Dr. Neuman's presentation was technology and border security. He began his presentation by indicating that because of the importance, in their view, of biometrics, the Department of Homeland Security is working on designing biometric research projects to advance their knowledge of its uses and applications in a security context. Further, he indicated that privacy concerns are taken very seriously by the Department, as demonstrated by the presence of a legislatively mandated senior privacy officer who advises the Secretary in charge of these projects.

Dr. Neuman continued by stating that in the White House, the National Science and Technology Council Coordinating Group on Biometrics, in conjunction with over a dozen other departments and agencies, is looking at a series of questions or issues relating to the use of biometrics, including:

- Physical and logical access,
- Biometrics audit and tracking within security systems,
- Immigration,
- Travel, and
- Related applications.

The set of tasks before the coordinating group is to identify gaps in the research and to ensure that these gaps are addressed. As well, the National Institute on Standards and Technology is conducting field accuracy testing of biometrics, while the Technical Support Working Group has funding for industry and is supporting a number of projects relating to the application of biometrics. Dr. Neuman indicated that it is this collection of agencies that is driving the agenda in the United States.

The Coordinating Group has organized the identified priorities into four working groups:

- Biometric modalities (fingerprints, irises, etc),
- Biometric systems and human interface,
- Biometrics fusion, test infrastructure and evaluation, and

- Social, legal and privacy issues.

Dr. Neuman indicated that this last group has been very active and successful. There are, however, in his view, a number of international issues that have not yet been addressed.

In regard to the suggestion that there is a trade-off between privacy and security, Dr. Neuman argued that it is not an either/or proposition. Privacy, in his view, is not synonymous with anonymity, and it is not something that can be derived from the inefficiency of the system. He defined privacy as the ability to exercise personal control over one's identity and how it is used. As such, he expressed the view that privacy is associated with the prevention of identity theft and control over the use of personal information. For Dr. Neuman, protecting privacy means being able to correct an error or prevent fraud associated with a suspected use or misuse of information by authorities. In this context, he provided an example of how a biometric can enhance privacy, such as when an authority looks something up in a system, and their authority to do so is also verified through the use of their own biometric identifier.

Dr. Neuman talked about the need for a "made in Canada" solution and cited, in this context, article 32 of the Manley-Ridge Accord on using joint research. In his view, one of the key issues that remains to be addressed is the use of biometric systems for personal privacy and common security. Article 32 of the Accord emphasizes both of these aspects and draws on what he sees as the inappropriate tension between the two areas of public policy.

Dr. Neuman concluded his presentation by suggesting some potential joint activities between the United States and Canada. He offered as an example follow up to a recent study sponsored by the White House on the accuracy of non-computer aided identification, which might serve as a baseline for future studies. He concluded by stating that the research community currently lacks a benchmark on the number of false accepts and rejects in the human systems of identification that are currently in use.

Gerry Van Kessel
Coordinator, Intergovernmental Consultations on Asylum, Refugee and Migration Policies in Europe, North America and Australia

Mr. Van Kessel is head of an intergovernmental secretariat in Geneva that deals with migration and asylum policies. Previously, he was an official of Citizenship and Immigration Canada. He began his remarks by indicating that he is not an expert on biometrics. As such, the focus of his presentation was on management and policy rather than the technical issues concerning the use of biometrics. He stated that the issue of the use of biometrics is too important to be left to the technologists and that one of the difficulties with technology is that it is an area of mystery and darkness for many managers.

Mr. Van Kessel outlined some current international examples of the use of biometrics. The use of biometrics is greatest at airports through processes called trusted travel facilitation or positive verification. Examples include CANPass at Vancouver International Airport and the INS (Immigration and Naturalization Service) Pass in use in ten U.S. airports. He indicated that there are biometrics applications in place in Singapore, Tel Aviv, Amsterdam, Zurich, Sydney and Sweden. Germany and the Netherlands are piloting biometrics in their visa issuance processes and the United States and the European Union plan to do the same. The United Nations High Commission for Refugees uses a system with Afghan refugees returning to Afghanistan from Pakistan and Italy that has a national identity card that uses biometric identifiers. The International Civil Aviation Organization has set international biometrics standards for travel documents.

In Mr. Van Kessel's view, the question is not whether to adopt biometrics, as it is too late to turn back the tide of biometric technology; rather the issue now is how to manage its applications?

The promise of the use of biometrics in the immigration context, as identified by Mr. Van Kessel, is that they:

- Offer a greater assurance of identity,
- Provide an identification for legal residents and refugees that is universally recognized,
- Facilitate refugee evacuations and repatriations,
- Help to counter fraud and abuses,
- Deter fraud in medical screening and in the case of individuals subject to health checks,
- Reduce the reward for non-compliance,
- Improve the identification of criminals and other risks, and
- Can serve as a unique identifier for improved case processing.

Mr. Van Kessel indicated that the use of biometrics is not simply a matter of realizing potential benefits. He also identified a number of associated challenges. These include:

- Human data entry errors,
- The possibility of malfeasance,
- Quality assurance, and
- The need for frequent training for the administrators of a biometrics-based system.

In his opinion, biometric technologies do not completely solve the problem of identity, as they can be fooled at the point of enrollment. The integrity of a biometric system depends on the quality of the enrollment process.

Mr. Van Kessel indicated that the problem of the protection of privacy requires that safeguards are put in place at the beginning of a system's design, in order to restrict data sharing, function creep and inappropriate data usage. It is his belief that biometrics need not subvert informational privacy. Biometrics can be privacy enhancing if systems are designed with that objective in mind. Another important consideration for Mr. Van Kessel was that all technologies do not have the same level of acceptance by the public, and often there is acceptance of a technology only if it has a perceived benefit. So an important question for Mr. Van Kessel was whether the delivery of a biometric system lives up to its promise of improved security. Does it deliver what it actually says it will? For example, will biometrics really facilitate border crossing?

He continued by talking about the relationship between biometrics and migration and asylum management. There are two categories of individuals who seek to enter countries: those who are allowed to and those who are not. An individual either meets the criteria regarding admissibility or does not. Central to being able to make this determination is confidence on the part of the decision-maker about the identity of the individual seeking to enter or remain in the country. Persons who meet the conditions of entry have no reason not to want to be identified, while persons who are refused entry may seek to create another identity that improves the chances of being allowed to enter or remain. They may be more hesitant to do so, in his opinion, if they know that a biometric identification method will be used to ascertain their identity.

Mr. Van Kessel indicated that there has always been fraud and misrepresentation in immigration, in particular in areas such as family reunification, refugee claims and students who intend to work. The

lengths to which individuals go in hiding their identities is astonishing. So the question emerges, how do you deal with people whose identity and intentions are unknown?

For many, being without documents is the best way to stay in Canada. Mr. Van Kessel indicated that over the past 20 years this has been a growing phenomenon, as have been the efforts of governments to respond to the various aspects of illegal migration, including the problem of documentation and identity. In his opinion, all countries face a challenge in creating documents that respond effectively to the challenge of counterfeiters.

Mr. Van Kessel stated that before September 11, 2001, immigration violations were often viewed as benign. Now, however, this view has changed. Failures in migration management can have serious consequences for public security and identification fraud is a tool of terrorists. So the question is how to identify the people who should be stopped while allowing the rest to travel as they wish? In his view, many elements have to come together to create an approach that works. Biometrics addresses this challenge as it holds out the best chance of identifying individuals and allows for the checking of verified identities against a central database.

Mr. Van Kessel concluded by stating that biometrics will enhance the ability of Citizenship and Immigration Canada officers to make confident and accurate decisions, and will allow for better and faster processing of individuals. When used appropriately, biometrics assist governments in managing the flow of people, however there is a great deal of work still to do before these technologies can be widely implemented.

Questions

Some participants expressed concern about the potential to develop a "we-versus-they" mentality in the implementation of a biometric card and that biometrics would tend to be used to facilitate privileges for the privileged and as a control mechanism for the least privileged. The panelists responded by indicating that, in general, there is support among the lesser privileged for the use of appropriate biometric cards, such as the application of biometrics to registration cards in the UK For some, cards are a way of securing benefits quickly and easily – not only is the process much faster with biometric cards, those with genuine claims usually want some kind of stable document showing their status. At the same time, cards can be used to protect genuine claimants by excluding the people who are not making legitimate claims.

Another point that was raised by a panelist was that there are no clear statistics on the extent of the abuse of the system by refugees, although stories of abuses can be found in every newspaper in the EU In her view, the use of biometric systems such as EURODAC, for instance, may be able to help dispel some of these myths by providing credible and accurate data. Finally, a third panelist indicated that there is a real policy issue in terms of how to balance the rights of refugees versus the right of a country to limit migration. The panelist stated that governments need to address the policy issues first and then move to the technical aspects.

A participant asked for some elaboration on the privacy oversight that takes place on the systems described by the panelists. A panelist responded by indicating that in the EU there is an independent European Data Protection Office, along with a series of independent national data protection offices. These offices conduct audits, and the data protection offices can follow up on transactions and specify how long an immigration office needs to keep archived data. A second panelist indicated that in the UK, there is a legal duty to comply with the *Information Protection Act*.

A final question concerned the potential to use border identification systems as vehicles to identify individuals for harassment or abuse by government. Again, the panel responded by pointing to the

potential for biometric systems to provide the opportunity to introduce objectivity into the process by taking the decision point about identification, or verification of identity, away from a guard or inspection officer and placing it with an impartial vehicle such as the EURODAC system.

One of the panelists summed up the question of the potential for national identity cards to be abused by asking rhetorically, whether there is a history of technologies exacerbating inequality. The answer, in their view, was negative, as biometric technologies give legitimate people easier access to the services they require while reassuring the rest of the public that abuses are being minimized. As to the question of whether technologies can be used for ill, the panelist responded that any technology can be used inappropriately, so it is important to take advantage of the current novelty and interest in biometrics to address fundamental questions of governance and control in order to minimize the potential for future abuse.

Luncheon Speaker – Frank Graves
President
EKOS Research Associates Inc.

The luncheon speech, given by Frank Graves, President, EKOS Research Associates Inc. (EKOS), consisted of a summary and analysis of recent work by EKOS on privacy issues and on the possible implementation of a biometric-enabled national identity card. The findings in the presentation were based on evidence from sixteen focus groups conducted by EKOS in the past year relating to privacy issues. The results are consistent with those from a general survey of 3,000 Canadians.

Mr. Graves' primary contention was that although opponents of a national identity card tend to be more vociferous than proponents, they are not the majority of Canadians. The research undertaken by EKOS indicate that, if the case is made clearly, the public would be open to the inevitability and plausibility of implementing a national identity card.

He continued by stating that while Canadians do have some trouble and concern with the idea of a biometric card, especially around issues of privacy and the competence of governments, these concerns are eclipsed by the clear problems they see with the current system, and other related considerations. In Mr. Graves' view, it is clear that this is not where Canadians were ten years ago. Polls conducted by EKOS in the early 1990s indicated that there was not nearly the same quality or quantity of concern.

Although Canadians feel that privacy is important and that it is under siege, they feel that they are capable of managing these threats. Indeed, concern about privacy has declined over the years and has been displaced by familiarity with new technologies. Citizens have also become less concerned as dire predictions of technological intrusion and catastrophic failures have not come to pass. Mr. Graves noted that although privacy concerns have declined substantially over the past few years, they have gone back up since September 11, 2001. He indicated, however, that although many of the attitudes toward privacy have returned to the levels exhibited prior to this event, security concerns have also remained very high for the Canadian public. At the same time, public confidence in who can take care of privacy issues has shifted away from the private to the public sector. In fact, faith in the public sector, in this regard, is increasing.

Mr. Graves asserted that the Orwellian caveat about the risk of privacy intrusions by "big government" is something that is having a diminishing impact on younger generations of Canadians. For the younger generation, the statement – "I do not mind governments using information if I know about it and can stop it" – elicited agreement from about 75 per cent of respondents. When the same question was asked using

the term "companies" in place of "governments", the level of support was about 71 per cent in 1992 and has now dropped to about 40 per cent.

Mr. Graves also indicated that Canadians seem to view the perceived dichotomy between privacy and security as being false. They do not see these issues as mutually exclusive and they will demand a high level of both. They are not convinced that bad things are going to happen, however, they also want to see what kinds of safeguards and measures are being put in place.

Another finding that Mr. Graves presented was that since September 11, 2001, many of the population effects that had manifested themselves previously have now dissipated, such as the opposition to immigration from various countries. There does, however, seem to be a permanent backlash against immigration from Arab countries and support for racial profiling. In many areas, such as the economy and feelings towards the state, opinions have returned to pre 9/11 levels, but effects on privacy and security concerns seem to be more permanent in nature.

With regard to Canadian perceptions of risk appraisal, such as the institution of airport taxes and surveillance cameras, they seem to be willing to make specific trade-offs. Consistently, Mr. Graves argued, Canadians seem to line up on the side of security, and yet they do not seem to be so concerned about the issue of terrorism in Canada. He indicated that there is also concern about the Canada-United States relationship, with 50 per cent of Canadians supporting the proposition that there is serious terrorist activity in Canada. Given that the support for a national identity card does not seem to be rooted in a sense that "bad things are going to happen to Canada", in his opinion, it becomes important to understand where the support for a national identity card is coming from within the Canadian population.

Polls undertaken by EKOS in the past year indicated that about 50 per cent of Canadians believe that the government is a pretty good steward of privacy and that it will not abuse the powers that it is granted, in contrast to 25 per cent who disagree with this statement. Mr. Graves stated that those who are critical, however, tend to be extremely vocal. In both Canada and the United States, there is a plurality of the population who believes that the police should be given more power. If this idea is presented in conjunction with the proposition that Canada needs to do this to fight against terrorism, a clear majority support more police or state power to fight terrorism.

Mr. Graves argued that the concerns about a national identity card seem to be mainly philosophical in nature – that the current generation of Canadians must not compromise the privacy of the next generation to protect their security. There seems to be very strong concern over the potential to compromise the civil liberties of the next generation of Canadians. With that in mind, security does not appear to be the main driver in support of a national identity card; it seems to be as much about the potential for abuse in the current system. Canadians are comparing the advantages of a biometric card against the perception of the kinds of abuses that have taken place with the current system.

Mr. Graves indicated that not only is there majority support for a national identity card, the more respondents learned about biometrics through the EKOS research, and the more they heard about the pros and cons of the card, the more they tended to strengthen their support for a national identity card. Only 6 per cent of Canadians think that the abuse of identity documents is not a serious issue.

A question was asked about the potential for a card to be either voluntary or mandatory in nature. Mr. Graves stated that anything that was voluntary tended to enjoy a higher degree of support than would a mandatory version of the same item, but not by very much. In focus groups, there was more support for a mandatory card because of the feeling that criminals and abusers of the system would not sign up for a voluntary card.

Mr. Graves asserted that when the idea of a biometric feature was presented in conjunction with the idea of a national identity card, it elevated support for the national identity card by a significant degree. For Canadians, the positive aspects of a national identity card are that it can reduce fraud and abuse, provide more accurate identification than that which currently exists, may help with security and might help to maintain access to the United States market. Some of the negative perceptions of the national identity card were in regard to privacy issues, cost, and concern around the potential for a 'slippery slope' effect.

To conclude, Mr. Graves indicated that the government needs a solid rationale for the implementation of a national identity card. Canadians need to understand how it will be implemented, why, what it is going to mean for citizens, and how is it going to work. The public also believes that it is inevitable that this is going to happen so the government might as well plan for it now. There is support among the public for the use of biometrics to reduce fraud and abuse in the system. At the same time there is still a great deal of concern about private sector applications such as the screening of applicants for work (commercial transactions are more of a concern for the public while public uses are less problematic).

In the end, Mr. Graves argued that about 80 per cent of the public think that the implementation of biometric technologies is inevitable. As such, there is strong support for the creation of improved identification documents, with a national identity card being seen as one of many possible vehicles. Currently, pragmatic arguments for such a card seem to trump philosophical arguments against. Few members of the public are actively calling for a biometric national identity card, but there is a general acceptance that such a card may be necessary and that the competence is there within the public service to deal with the privacy issues, should there be a compelling need.

In the discussion, some of the participants expressed concerns about the study and its methodology, citing a methodological slant towards security, the use of biometrics and the impacts of terrorism. They suggested that perhaps technology is not the only solution. Mr. Graves responded to these concerns by agreeing with the caveat about the overuse of technology as a solution. Indeed, he stated that when Canadians were asked how Canada should deal with terrorism in the long term, the top two choices were better forms of intelligence and developing a more multi-cultural and tolerant society.

Afternoon Speaker: Privacy Issues – Stephanie Perrin
President
Digital Discretion Company Inc.

Ms. Perrin began her presentation by stating that she would focus on the privacy issues related to a national identification card, rather than get into the technology. One of her principle points was that there was a rush after September 11, 2001 (9/11) to bring forward technologies that had been 'in the hopper' prior to this event, but for which previously there were no markets. In the wake of 9/11, in her view, such issues as access by law enforcement to personal data, and other aspects of due process have been eroded to the extent that technologies which are extremely damaging to individual privacy could be introduced more broadly and in a number of contexts.

Fundamentally, in the view of Ms. Perrin, there is a need for free speech if democracy is to survive. Although she agreed with Mr. Dershowitz's point from the evening before that relying on the frailty of technology is a fool's course, she stated that there is currently an important debate in civil society over the most appropriate course of action to take on these issues. She stated that the people who criticize the development of a biometric card are not just human rights activists; they are also security and technology experts.

One of Ms. Perrin's major contentions was that rushing to a solution without defining the problem is foolish. Given this contention, she posed the question as to why Canada is rushing to the use of biometrics as a solution. In the border control context, it is a logical step, but in many other instances it may not make sense. Questions need to be asked such as: Are we authenticating individuals? Are we verifying their identity? Are we asking for identity when an anonymous but secure card could serve as well? In her view, there are many ways of dealing with the challenges of identity theft, such as clamping down on easy credit and other steps that privacy advocates have identified. As such, there is no need to implement anything as privacy-invasive as a national identity card.

Canadians, according to Ms. Perrin, have to put the issue of a national identity card in the context of what is happening in the marketplace, given the appetite for transactional data. Ms. Perrin posed the question as to whether the market should be permitted to exercise an uncurbed demand for data. She identified the failure of oversight mechanisms as a primary concern in the implementation of biometric systems. Privacy legislation alone will not protect privacy, she asserted, as the gathering of data causes a problem unto itself and oversight bodies are under-resourced, and they do not have the technical capability to fulfill their roles in protecting citizens in the context of high tech security solutions. She was also concerned that a national identity card will be under-resourced in its implementation; while there are theoretical ways to solve privacy problems they cost money, and the money will likely not be there when the systems are actually built. Furthermore, the cards will be loaded with other applications.

Ms. Perrin suggested that it is dishonest to discuss the issue of a national identity card as anything but a system, existing on a continuum. Canada is embarking on this journey toward a national identity card without first undertaking adequate research. Further, she suggested that the right to privacy is situated in a matrix of associated rights in the Charter of Rights and the Universal Declaration of Human Rights, and other fundamental rights such as freedom of movement and freedom of association are also under threat from a national identity card.

Following this discussion of the relationship of a national identity card to various types of rights, Ms. Perrin looked at the concept of a national identity card from the perspective of ten privacy principles. She stated that accountability is very important, purpose specification is also very important, but that consent is not a realistic expectation in regard to an identity card. She went on to state that voluntary cards tend to become non-voluntary very quickly, which compromises the principle of individual consent. Accuracy is a two-edged sword, as it can be used to compromise individual privacy, which is why sometimes privacy advocates like to see the collection of 'sloppy data', since fewer people can then rely on them for new purposes.

The principle of access was seen by Ms. Perrin to be critical, since an individual has to be able to see and challenge the data that is in these systems if he or she is able to guarantee data integrity. She noted that in Canada an individual does not even have to be the subject of data to challenge its collection and codification in databases under the Personal Information Protection and Electronic Documents Act. This provision specifically addresses the fact that often only the people who are experts in security or systems are able to see what is happening to personal data.

Ms. Perrin stated that there is a fundamental characteristic of biometrics which alarms many people: they pertain to the body. Similarly, biometrics cannot be revoked if they are compromised. Revocation is a key problem and challenge for any authentication system, but especially biometric systems. If the bitstream is compromised, the biometric system will have to permit re-registration of the true individual. One of the big challenges with identity theft right now, she contended, is how does an individual get his own identity back once it is compromised? If a biometric system is compromised, then it is much harder to change the system to re-establish an individual's identity.

Ms. Perrin expressed concern that citizens would be asked for a national identity card as identification in a steadily increasing number of commercial transactions. At the moment, we have an existing problem with the Social Insurance Number, where individuals are asked to produce their SINs at a grocery or Blockbuster video stores. All commercial establishments are looking for secure ID now, and this problem would only be exacerbated through the implementation of a biometric identity card. She stated that in a democracy, there are often citizens who have very little understanding of their rights, and therefore it behooves the government to pay particular attention to ensuring that these rights are not violated.

A further issue that Ms. Perrin identified was the massive costs associated with the implementation of a national identity card. The cost increase would not be arithmetic in nature but rather would increase exponentially with a larger enrollment group. Further, she asserted that the entire concept of oversight is very important and the examples cited of cards in Europe neglect the fact that Europe has an infrastructure of oversight, including the European Court of Human Rights, Universal Data Protection Law, and independent Data Commissioners. We do not have such oversight in Canada. This, in her view, calls into question the ability of the government to implement effective independent oversight of the development and implementation of a national identity card.

For Ms. Perrin, the issues of sovereignty, access to and control of data were also significant. She indicated that for a system to be secure there must be both access and human controls. As an example, she asked the rhetorical question of what would happen if Canadian data are housed in India – is it possible to ensure that the individuals handling Canadian data in India meet Canadian standards of integrity? What rights would foreign governments have to access the data? The answer is simple: all governments have rights to access and collect data from data systems that trump individual privacy rights. Given that very large amounts of sensitive data could be accessed through a national identity card that yields transactional data, choices with respect to technology and data storage and management become extremely important. In her view, the right policies and laws to protect data are necessary but not sufficient; there must be limits to data collection.

Ms. Perrin concluded her presentation by making some suggestions on how to achieve progress in the debate over biometrics. She identified the need to:

- Start a regular dialogue with civil society.
- Find the problems, sketch them out and develop an analytical framework.
- Stop promising a safe world to the public. The premise that giving up privacy can make someone safe from terrorism is a lie. We live in an unsafe world and governments have a responsibility to convey that fact to citizens.
- Provide effective oversight.
- Provide more transparency.
- Do the research.

During the discussion that followed Ms. Perrin's presentation, a participant stated that many Canadians will have biometric cards in the near future and that it is very clear that the rest of the world is moving toward this solution. As such, Canada has some clear options – do nothing or proceed to develop a "made in Canada" solution. Canadians are concerned about function creep and the need for firewalls, but many individuals already use biometric technologies and with knowledge and more information their fears of these technologies subsides.

In response to these assertions, Ms. Perrin indicated that there is a limited ambit in which to carve out a "made in Canada" solution. She stated that one could argue that some groups such as truckers might have a higher acceptance threshold for the use of biometrics than others but that this should not mean that the same standard is applied in every situation. She concluded by stating that the use and collection of data should be appropriate to the situation for which the data are required.

Another participant concluded this portion of the session by stating that there is really a four-part test for the protection of privacy:

- That there is a specialized data protection regime in place,
- Independent oversight,
- The use of privacy impact assessments, and
- The adoption of as many privacy enhancing technologies as possible.

Panel Session 2: Biometrics - Understanding and Assessing the Implications

Dr. Roger Gibbins, President and Chief Executive Officer of the Canada West Foundation

Jennifer Stoddart, Présidente, Commission d'accès à l'information du Québec

Raj Nanavati, International Biometrics Group

Raymonde Folco, Member of Parliament, Laval West

The afternoon panel focused on understanding and assessing the implications of biometrics in the context of a national identity card in Canada.

Roger Gibbins
President and CEO of the Canada West Foundation

Dr. Gibbins began by stating that post 9-11, and in terms of concerns over identity fraud, the use of biometrics seems desirable and useful. As such, his comments addressed two primary topics:

(1) The need for a new national identity card as opposed to the incorporation of biometrics into existing cards, and

(2) Implementation issues

He also indicated that he would focus on the national identity card and not on biometrics more generally. He began by stating that the incorporation of biometrics in a national identity card seems to be less controversial that the implementation of the card itself. For him, the question seems to be - why do we need a third platform for establishing identity? The need does not seem to be intuitive or obvious. An updated passport could be used to travel, so the implementation of an ID card seems to imply the need for biometric identifiers within a domestic context. So what does the government of Canada have in mind? When will Canadians need to produce their card and to whom?

Dr. Gibbins questioned whether the national identification card would be like a passport that could be left at home or like a driver's license that is kept close at hand. He cited the Social Insurance Number as an example of the dangers of function creep, where the Canadian public was assured that it would be used only for a limited purpose while it was soon adopted by the private sector. As such, he stated the belief that any identification card would soon move from public sector applications out into the private sector.

In his view, a new national identification card would soon become a master platform for the public and private sphere, the new gold standard for private and public transactions. He stated that this may indeed become necessary for some transactions. The challenge, in Dr. Gibbins' view, is to make sure that the information is not abused and that the public will not think that it will be used against them at any point. He pointed to the challenge of the Orwellian caveat in terms of the dangers of the misuse of information.

He used the example of the grimness of the new policy that all passport pictures must not feature a smiling individual as an issue that can be dismissed on technical grounds, but not on a political level. Thus, while the introduction of biometrics may be inevitable, in his view the use of a national identity card is not.

Dr. Gibbins also saw the issue of the voluntary versus mandatory nature of the card as being problematic. If the population coverage of a new card were limited, it could become a vehicle for stigmatization and privilege. It could be a badge for the business class or part of the stigmatization of new immigrants. In summary, in his view the card would not be useful unless it was mandatory

Another issue for Dr. Gibbins was the issue of who would pay for the new cards. If it is the users, he thought that the cost would reinforce existing class divisions. He indicated that the overall cost of the implementation of a card was also an issue and that the financial estimates on the costs of implementation should not be believed. He was also concerned that the residents of marginal areas of the country will be outside the coverage of the new card. A final issue he raised was that of the types of information that will be displayed and why on the new cards. Will this information migrate to the private sector? In his perspective, even if the information is protected from function creep into the private sector, the public will still view the card as a link to other functions. The assertion of effective firewalls will not be trusted or believed.

For some, in the opinion of Dr. Gibbins, the implementation of a national identity card will be perceived like the gun registry. He did state, however, that it is not clear how Canadians will react to a biometric card as part of the immigration system. He indicated that there may be more support for the implementation of more extensive documentation on a them-versus-us basis. In many respects, for Dr. Gibbins, the value of the card will hinge its level of integration and inter-operability with the US homeland security provisions. If it is fully integrated, he thought that Canadians would be worried about the flow of information to the U.S., given the current popular resistance to the flow of information to the US. For the implementation of a national identity card to be successful, therefore, he stated that these issues must be solved and addressed up front.

In Dr. Gibbins' view, part of the rationale for a national identity card is fear about new kinds of security threats that may emerge for Canadians in the future. Dr. Gibbins asked, however, whether the need for enhanced security will continue to trump other concerns in the future.

Dr. Gibbins asserted that one way to sell Canadians on the idea of a national identity card is the notion that this card could be the solution to the challenge of carrying multiple cards. If Canadians can use this card to do everything that multiple cards can currently do, then they may be more supportive of its implementation. The development of such a 'super' card, however, would reinforce the deep misgivings that Canadians already have about the surrender of information to the commercial sector.

Dr. Gibbins concluded his presentation by indicating that there may be some real advantages to taking an incremental approach to the implementation of biometrics.

Jennifer Stoddart
Présidente
Commission d'accès à l'information du Québec

Ms. Stoddart began her presentation by indicating that the issue of the use of biometrics in the context of identity verification has been included in a specific law in Quebec for some time: la Loi concernant le cadre juridique des technologies de l'information. Indeed, she stated that historically, in Quebec, particular care has been given to the protection of individual information in general; for example in 1982, the National Assembly adopted the first law concerning the protection of personal information in Quebec. It is during this initiative of the Quebec government that the use of biometrics was first examined. Indeed, following the events of September 11, the enthusiasm concerning biometrics confirmed the choice of the Quebec government to legally regulate their use.

Ms. Stoddart stated that the *Commission d'accès à l'information du Québec* has always expressed reservations about a national identity card. Discussion first arose in Quebec as a result of concerns about potential electoral corruption in some ridings during the 1990 provincial election, and the question was raised as to the feasibility of an identity card for Quebec. The Commission has opposed this and later proposals for a universal identity card and instead has supported a number of other methods of verifying identity that have since been successfully implemented.

La loi concernant le cadre juridique des technologies de l'information du Québec has particular provisions in its legislation that allow the Commission to monitor and control databases of biometric characteristics and measurements. The objective of this legislation is to provide a framework for the use of this information, in particular to provide a measure of protection for electronic transactions, to standardize legal documents and to create a functional equivalence between electronic and paper documentation. In some of these contexts, the issue of authentication becomes a challenge, and Ms. Stoddart recognized that the use of this information on the Internet poses a challenge under Quebec's system of civil law. There are also particular sections in the Quebec legislation that deal specifically with the use of biometrics as a tool for personal identification.

Biometrics are authorized for linking individuals and documents under three conditions:

1. Biometric identification cannot affect the physical integrity of the individual.
2. It cannot be used to link an individual and a location, except for reasons of health and safety.
3. There must be express consent provided by the person concerned and only for purposes of verification and confirmation of identity.

While these provisions have not been tested in court, they are in the context of broader legal protections in Quebec for personal privacy, including that the legal system in Quebec cannot compel anyone to provide a sample of bodily fluid, cannot use a device to find someone, and cannot use a locating device to track an individual.

Ms. Stoddart stated that in Quebec, the use of biometric characteristics for an application would have to pass the test of necessity – requiring a minimum of biometric characteristics – and no recording could be carried out without the knowledge of the individual. The fact that the police lift fingerprints without consent would not serve as a basis for further use of biometric identifiers. Any biometric information that is collected cannot also be used for any other type of decision or purpose, except for verification or confirmation (for example, a drug test could not be conducted on the basis of biometric information collected for an authorized use).

For Ms. Stoddart, another important feature of the Quebec legislation is that information must be disclosed to subjects upon request and biometric identifiers will be destroyed when their purposes have been met. One of the most innovative elements of the legislation is, in her view, the requirement that the existence of all databases of biometric identifiers must be disclosed to the *Commission d'accès à l'information du Québec* – before they become operational and even if they are not in use.

In describing the Commission's powers with respect to databases of biometric identifiers, Ms. Stoddart indicated that they are actually quite limited – it may impose orders on databases with respect to their design and it can suspend a database. The Commission prefers, however, to rely on a self-analysis kit for database administrators and on a privacy impact assessment tool. So far, she stated, there have only been four cases of such databases being developed and implemented in Quebec, most notably: a voluntary database at the University of Montreal athletic centre; a database in a unionized workplace, which raised the issue of the union's ability to provide consent on behalf of its members; and a small biometric database

used in a Hydro Quebec pilot project, which verifies the identity of individuals making large-scale financial transactions.

In conclusion, Ms. Stoddart stated that in Quebec the use of biometrics is seen in the context of privacy rights, which are recognized as a fundamental right and a priority concern for legislators. She argued that for governments that want to implement biometric databases and tools, strict rules should be in place, including that the system must be ultra-secure and its development and use must be compatible with human rights legislation and other privacy principles. Finally, she stated that the Quebec system should be a model for all of Canada and in particular that any initiative must have an expert oversight function from an independent source, such as the *Commission d'Accès à l'information du Québec*.

Raj Nanavati
Partner
International Biometric Group

Mr. Nanavati began his presentation by stating that his firm developed a bio-privacy framework in 1999, in response to requests from clients, and to other indications that there was a need for a privacy framework that specifically addressed issues relating to biometrics. As such, this model ensures that privacy concerns are incorporated at the outset in biometric applications. He indicated that in the past his company has been consulted on the development of the Ontario Health Care Card, which has 12 million users, and by the White House on the Office of Science and Technology Policy on the US Smart initiative, which will involve more than 300 million users. If many individuals are using system such as these, it is vital to adhere to specific privacy and other policy requirements.

The first issue, in his mind, is to define how biometrics relate specifically to privacy concerns. In general, there are two types of privacy – personal privacy and informational privacy. So, should policy-makers consider biometric information to be personal data? In Mr. Nanavati's opinion, since a fingerprint does not provide any information about the individual from which it is taken, a very narrow interpretation could be to conclude that biometrics are not personal data. He indicated that it is often useful, however, to take a broader view of these matters and to look at privacy issues in a wider context.

Mr. Nanavati then discussed the importance of templates. He stated that in particular it is important to know how a template differs from an image. It is extremely important to know what type of image someone is looking at. An image can be related to someone on a one-to-one basis, while a template involves a one-way shift to create a unique signature that is different from the person's image. So, the use of templates, in Mr. Nanavati's view, mitigates some of the concerns about the misuse of data.

Another idea introduced by Mr. Nanavati was that the use of small systems is an important way of protecting privacy. While images are interoperable, templates, for the most part, are not. Since they are not interchangeable, a given technology deployment ties a customer to that one vendor's technology, which limits the ability of outside parties to read or interpret this information. The implications for privacy, in his view, are profound.

One challenge identified by Mr. Nanavati was that biometric data can change over time, so an important issue is how to measure the accuracy of biometric technologies. He indicated that there has been considerable work on scientifically and rigorously evaluating these technologies, given that they are in use by hundreds of millions of individuals. There are three primary errors that can be made by a biometric system: the false match, false non-match, and failure to enroll. He indicated that if a substantial number of people cannot enroll in a system, then it is necessary to have a back-up form of identification and the entire purpose of the system is compromised.

Mr. Nanavati stated that if there is very strict oversight of the enrollment process, then there will be a lower rate of failure to enroll. If, on the other hand, a self-serve kiosk is chosen to enroll the population in a system – a methodology with a high enrollment rate – it could lead to a 10 per cent failure rate. Thus, accuracy rates are based on technologies and specific deployments. He considered that there will always be people who cannot use a particular identifier, for example a small percentage of people do not have a consistent iris and so cannot effectively enroll in an iris scanning technology. So biometrics are not perfect, and there will always be some rate of false match. Mr. Nanavati indicated that the comparison that should be made, therefore, is whether the biometric improves on the existing system's failure rate. For example, in immigration applications, it is important to make sure that biometric failure rates are lower than those for visual matching.

Mr. Nanavati continued by stating that there are four identifiers which are used to evaluate a technology – whether it is privacy invasive, neutral, sympathetic, or protective. Government programs should have 'privacy-sympathetic' as a base-line requirement. In this context, he presented the three primary BioPrivacy functions, as identified by his firm:

- Analysis of biometric applications – impact framework
- Analysis of core technologies – technology risk, and
- Moving toward a privacy sympathetic system – best practices

He asserted that the use of these criteria in evaluating a biometric application ensures an objective framework for evaluation. He used the example of facial recognition technology at the Superbowl as an example of what can go wrong when these technologies are not applied in a consistent manner. At the Superbowl, there were numerous problems with the use of biometric technologies, such as a lack of informed consent on the part of participants – an impact which could potentially have been mitigated by signs that indicated that smart cameras were in use. In Mr. Nanavati's view, it is important to explain to people what is really going on and what the information that is being collected will be used for.

Mr. Nanavati stated that there is considerable confusion about what the term 'biometrics' really means. Some of the focus groups which Mr. Nanavati's organization has been conducting have been enlightening in this regard. In general, people linked fingerprint technologies with the police. After people used a fingerprint system first hand, there was a much higher rate of enrollment, which indicated that they were more likely to accept a biometric identifier once they had first-hand experience with its application. Verification and enrollment can be very simple if done properly. It seems that people need the real-world experience of using biometric applications to really evaluate the feasibility of this technology.

Mr. Nanavati stated that the BioPrivacy framework looks at a number of factors including:

- Optional or mandatory enrollment,
- Overt or covert use of the technology,
- Use for verification or for identification,
- Fixed duration vs. unlimited durations,
- Private sector vs. public sector,
- Individual vs. employee,
- User ownership vs. institutional ownership of data,
- Personal storage vs. template database,

- Behavioural vs. psychological biometric identifiers, and
- Template vs. identifiable data.

He stated that, using combinations of these factors, his firm creates technology risk ratings for various applications.

To conclude, Mr. Nanavati indicated that biometrics could not have done anything, in and of themselves, about the events of September 11, 2001. An identification system in which biometrics are an element could have allowed law enforcement agencies to compare data with criminal or terrorist watch lists. Currently, however, there is not a sizable bank of terrorist signatures or irises, so it is important to consider the use of such technologies closely in an anti-terrorism context.

Raymonde Folco
Member of Parliament, Laval West

Madame Folco began her presentation by differentiating between a principles-based and a more rules-based approach to biometrics. She stated that a rules-based approach lists the social ills to be addressed such as identity fraud, terrorism, and abuse of the system, while a principles-based approach focuses on values. Taking a rules-based approach opens the government to extensive risk. Instead of focusing on statements such as "If we do not break the law, we are within our rights and obligations," Madame Folco posited the view that the government should be looking at the rights of all affected parties. We should be asking, "Which course of action advances the common good, supporting trust, transparency and good governance?"

She went on to identify some of the fundamental architecture that supports the Canadian state such as the *Charter of Rights and Freedoms* and guarantees in the Canadian Constitution. Some of these rights have been curtailed with new security measures. At the same time, new legislation such as the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) and provincial privacy acts also protect citizens' rights to privacy. From this starting point, there are three themes that need to be addressed: security, privacy and human rights, and the relationship among them. In her view, the important question to ask is: what rights do the affected parties have and which approach respects these rights? The more serious the potential for the invasion of these rights, the worse is the course of action.

Madame Folco stated that much of the recent focus in the debate about biometrics has been on security, and that the Biometrics Forum would have taken place even without the events of September 11, 2001. In this world of post-Cold War, open détente and collaboration, Canadians will have to deal with non-state sources of terrorism and identity theft. Economic and social progress is linked to the increased mobility of people, which is linked, in turn, to the ability to prove one's identity. So, she asked, in a new security-conscious environment, what are the new risks and the ongoing risks, and where does this issue of biometrics fit in?

With respect to privacy, Madame Folco asked whether enough was being done to inform Canadians of their choices. Is technology an instrument or a means to an end? Is privacy a value to be protected or a state to be achieved? Thus far, biometrics have been seen as either an unqualified threat or as an enabler of privacy. But, she asked, is the government outlining for Canadians the full scope of each option? Which course of action treats each person the same way, supports fairness and justice, and allows citizens to make their own decisions and to affect their own lives? Does information from polls provide a sound basis for action? What about the silent majority – what representation of the citizenry reflects the actual views of the population? How necessary are polls as a reflection of public opinion? Citizen advocates seem to be

saying 'no' to a national identity card, but how inclusive or exclusive are these groups? Whom do they represent? Ultimately, what is the public willing to compromise in order to get something else? This is an important question in the application of a national identity card. In her view, the facts must be on the table so that citizens can make an informed choice.

The issue of human rights is also important and raises three key issues: Are there differential impacts on different groups (for example, on religious groups)? What kind of society does this encourage? What tools are available to limit differential impacts?

Madame Folco concluded by asking which course of action affects the common good? In her view, the question that must be asked is: Do Canadians have the honesty, courage, compassion, fairness, self control and prudence to confront the real threat of terrorism in Canada without moving to racist generalizations? Does Canada need a new biometric lens in order to assist officials in situations where a purely objective indicator is useful? What is the point of privacy legislation and PIPEDA, and what is the point of a Charter if people cannot feel safe at the same time their privacy is being protected?

So the question remains, does Canada need to incorporate a principles- or a rights-based approach to a national identity card? In Madame Folco's view, any move to adopt biometrics will be an enhancement only if principles and ethics are integral to the approach that is taken and enshrined at each stage of the process. Canada must look at human dignity and worth, assess the product being offered, and examine its benefits versus its costs and its benefits versus its risks. Legislation must protect Canadians. Madame Folco finished her presentation by stating: "Let us control technology instead of technology controlling us."

Questions

Participants began their dialogue with the panelists by asking about the claims that biometric technologies are not yet 'there' in terms of their delivery. One of the panelists responded by stating that this all depends on the need for accuracy – which in turn depends on the deployment. As an example, New York City has been using fingerprint technology to identify welfare recipients for several years. Using facial recognition in airports has not been effective because the technology did not identify terrorists. The technology was deployed in such a way, however, that it was taking photos from 20 feet away with shadows and movement affecting its accuracy. There are some deployments where this technology does not work. You need to look at each deployment on its own and figure out if it makes sense or not.

Another participant suggested that it is necessary to have ongoing independent auditing of some of the intrusive powers that have recently been enacted by government. The panel responded by stating that currently the Treasury Board Secretariat of Canada submits every government project having an impact on privacy to the Privacy Commissioner, and this oversight should be expanded more explicitly in the private sector. Another panelist indicated that parliament responds to what Canadians want, so eventually there will need to be a hard look at the privacy legislation and its impact on issues of verification and authentication.

A final participant asserted that there had been a lot discussion at this session of the use of biometrics for the purposes of matching refugees and asylum seekers. He stated that as a Canadian citizen, he is not coming to the border seeking entry, but is still being told that there is a need for an identity card that can be implemented in a domestic context. He did not feel that the case had been made for such a card. One of the panelists responded by stating that this is a very important point. She indicated that the Biometrics Forum is an initiative of the Minister of Citizenship and Immigration Canada, who has the federal lead on document integrity issues. She concluded that someone had to raise the subject because it had not yet

been discussed. However, in the future, a broader group from across the country, including other levels of government and citizens in general, will have to determine what they want in terms of an identity policy.

Conclusions and Directions for Future Action – The Honourable Denis Coderre Minister of Citizenship and Immigration

The session concluded with remarks by the Honourable Denis Coderre. Minister Coderre began by reiterating his opening remark that this issue is very important both nationally and internationally. He noted that several members of the House of Commons Standing Committee on Citizenship and Immigration had attended the Forum, which he felt had "broken the ice" on a national debate.

Mr. Coderre stated that the use of biometrics is a fundamental issue affecting all Canadians. Citizenship and Immigration Canada has taken a lead in opening up a national debate because it has the lead within the federal government on foundation documents, including citizenship documents and the Permanent Resident documentation (the new Maple Leaf Card). The Minister asserted that biometrics are in use now and they are here to stay. It is not so much a question of "if" but rather of "when." Given the inevitability of this eventuality, Minister Coderre indicated that Canada needs to begin to think about and debate this issue; that the issue of a national identity card needs to be discussed in living rooms across the nation. He indicated that he did not see biometric identifiers as being only for landed immigrants and permanent residents but rather for all Canadians.

In Minister Coderre's view, identity theft, border security, and international standards are all reasons for examining biometrics. It is a Canadian question that requires a balanced approach, but the status quo is not an option. He felt a number of necessary conditions were in place: a strong privacy regime and good institutional working relationships in the privacy field. He liked the Quebec model of providing legislative safeguards for authorized uses of biometrics, because it responds to current realities. As the responsible Minister, he is obliged to cover all the angles and to look at all the possibilities. The national debate has begun and should continue.

Minister Coderre stated that Canada must ensure that its documents are secure without jeopardizing the privacy and values of Canadians. In the next five years Canada will need a million qualified workers and by 2026 demographic growth will be solely on the basis of immigration. He asserted that Canada needs to guarantee the integrity of our foundation documents and protect the identities of our citizens, in order to meet the challenges of this new wave of immigration. At the same time, he recognized that this subject is complex and that the government will have to put in place templates and strategies for firewalls in order to protect privacy while also enhancing security.

In pointing to the evolving nature of the issue, Minister Coderre gave the example of the use of picture identification which, many years ago, was quite controversial. Now, he asked Forum participants to imagine getting on an airplane without a photo ID. He stated that we, as a country, truly have to take a look at the collection of information and the uses of databases. The Biometrics Forum was only the beginning and there will be other steps, but it was a good start. He also looked forward to the final report of the Standing Committee on Citizenship and Immigration. In the final analysis, Canadians will adapt themselves and find a "made in Canada" solution within the global village.

ANNEX II: AGENDA

Tuesday, October 7, 2003 (Fairmont Chateau Laurier Hotel)

TIME	EVENT
5:15	**Registration**
5:30	**RECEPTION**
6:00	**DINNER**
7:20	**Opening Event Speech:** *Balancing Security and Civil Liberties* Professor Alan M. Dershowitz Professor of Law Harvard Law School

Wednesday, October 8, 2003 (National Arts Centre)

7:45	**Registration**
8:20	**Morning Announcements**
8:40	**Opening Remarks** The Honourable Denis Coderre Minister of Citizenship and Immigration
9:00	**Keynote Speaker** Dr. Colin Soutar Chief Technology Advisor Canadian Advanced Technology Association - Biometrics Group Chief Technology Officer Bioscrypt Inc.
9:45	**Instant Survey - Session 1**
10:00	**BREAK**
10:20	**Panel Session 1: Biometrics in the International Context** Martin Giles, Assistant Director United Kingdom Immigration Services Gillian Russell, Directorate General, Justice and Home Affairs European Commission Dr. W. Russell Neuman, Senior Policy Advisor White House Office of Science and Technology Policy Gerry Van Kessel, Coordinator Intergovernmental Consultations on Asylum, Refugee and Migration Policies in Europe, North America and Australia
12:00	**LUNCH**

12:50	**Luncheon Speaker** Frank Graves President EKOS Research Inc.
13:30	**Privacy Issues** Stephanie Perrin President Digital Discretion Company Inc.
2:00	**Panel Session 2: Biometrics – Understanding and Assessing the Implications** Dr. Roger Gibbins President and CEO Canada West Foundation Jennifer Stoddart Présidente Commission d'accès à l'information du Québec Raj Nanavati Partner International Biometric Group Raymonde Folco Member of Parliament, Laval West
3:30	**BREAK**
3:50	**Instant Survey – Session 2**
4:05	**Table Discussion and Dialogue**
4:45	**Where do we go from here? Closing remarks by the Honourable Denis Coderre**
5:00	**End of Forum**

ANNEX III: REGISTERED PARTICIPANTS (AS OF OCTOBER 6, 2003)

Hon. Denis Coderre, P.C., M.P.
Minister of Citizenship and Immigration Canada

Diane Ablonczy
M.P., Calgary-Nose Hill

Reg Alcock
M.P., Winnipeg South

Ken Anderson
Office of the Information and Privacy Commissioner/Ontario

Jahanshah Assadi
UN Commission for Refugees - Canada

Sarkis Assadourian
M.P., Brampton Centre

Rivka Augenfeld
Table de concertation des organismes au service des personnes réfugiées et immigrantes

Bill Bergen
Information Technology Association of Canada

Fariborz Birjandian
Alberta Association of Immigrant Serving Agencies

James Bissett
Public Commentator

Dr. Anu Bose
National Organization of Immigrant and Visible Minority Women

Sam Boutziouvis
Canadian Council of Chief Executives

Robert Bouvier
Teamsters Canada

Brion Brandt
Transport Canada

Patrice Brunet
Quebec Immigration Lawyers Association

John Bryden
M.P., Ancaster-Dundas-Flamborough-Aldershot

Mike Buisson
Royal Canadian Mounted Police

Rose Bullock
Alberta Government Services

Tony Cannavino
Canadian Police Association

Marc-André Charlebois
Association of Canadian Travel Agencies

Anna Chiappa
Canadian Ethnocultural Council

Peter Clark
Standards Council of Canada

Prof. Andrew Clement
Faculty of Information Studies
The University of Toronto

Graham Cooper
Canadian Trucking Alliance

Irwin Cotler
M.P., Mount Royal

Michelle d'Auray
Treasury Board Secretariat

Madeleine Dalphond-Guiral
M.P., Laval-Centre

Raymond D'Aoust
Office of the Privacy Commissioner of Canada

Bob Davidson
International Air Transport Association

Michel d'Avignon
Solicitor General of Canada

Janet Dench
Canadian Council for Refugees

Prof Alan M. Dershowitz
Harvard Law School

Bonnie Diamond
National Organization of Women and Law

Michel Dorais
Citizenship and Immigration Canada

Roland Dorsay
Canadian Airports Council

Ward Elcock
Canadian Security and Intelligence Service

Barry Elliott
Ontario Provincial Police

Warren Everson
Air Transport Association of Canada

Dr. David Flaherty
Privacy and Information Policy Consultant

Jean-Guy Fleury
Immigration and Refugee Board of Canada

Raymonde Folco
M.P., Laval West

Joe Fontana
M.P., London North Centre

Bridget Foster
Atlantic Regional Association of Immigrant Serving Agencies

Dr. Roger Gibbins
Canada West Foundation

Martin Giles
UK Immigration Services

Frank Graves
EKOS Research Associates Inc.

Roy Gray
Indian and Northern Affairs Canada

Art Hanger
M.P., Calgary Northeast

Jonathan Hatwell
Delegation of the European Commission in Canada

Ryan Higgitt
Student

Peter Hope-Tindall
data Privacy Partners Ltd.

Martin Huddart
International Biometric Industry Association

Thelma Johnson
Vital Statistics Council of Canada

Catherine Johnston
Advanced Card Technology Association of Canada

Onno Kremers
Human Resource Development Canada

François Laporte
Teamsters Canada

John Lawford
Public Interest Advocacy Centre

Anne Legars
Shipping Federation of Canada

Sophia Leung
M.P., Vancouver-Kingsway

Alfred MacLeod
Citizenship and Immigration Canada

Inky Mark
M.P., Dauphin-Swan River

Robert Marleau
Office of the Privacy Commissioner of Canada

Robert Martel
Inuit Tapiriit Kanatami

Gordon Maynard
Canadian Bar Association

Kathryn McCallion
Department of Foreign Affairs and International Trade

Steve McCammon
Canadian Civil Liberties Association

Gary McDonald
Department of Foreign Affairs and International Trade

Kevin McGarr
Canadian Air Transport Security Association

Paul McGrath
Canadian Bankers Association

Michael N. Murphy
Canadian Chamber of Commerce

Raj Nanavati
International Biometrics Group, LLC

Dr. W. Russell Neuman
The White House

Massimo Pacetti
M.P., St Léonard-St Michel

David Paterson
CATA Alliance

Chantal Péan
Canadian Tourism Association

Bill Pentney
Citizenship and Immigration Canada

Stephanie Perrin
Digital Discretion Company Inc.

Thao Pham
Privy Council Office

Jim Phillips
CAN/AM Border Trade Alliance

Jerry Pickard
M.P., Chatham-Kent-Essex

David Price
M.P., Compton-Stanstead

Yves Prud'Homme
Fédération des policiers et policières municipaux du Québec

James Puleo
International Organization for Migration

Hon. Robert K. Rae, P.C., O.C., Q.C.
Goodmans LLP

Raj Rasalingam
Pearson-Shoyama Institute

Glenn Robinson
Privy Council Office

Gillian Russell
European Commission

Gerry Salembier
Finance Canada

Ravi Sall
Citizenship and Immigration Canada (Youth Network)

Dr. Marc Saner
Institute on Governance

Dr. Colin Soutar
Bioscrypt Inc./CATA Alliance

Johanne St-Cyr
Canadian Council of Motor Transport Administrators

Valerie Steeves
Carleton University

Jennifer Stoddart
Commission d'accès à l'information du Québec

Tamy Superle
Student

Roch Tassé
International Civil Liberties Monitoring Group

Maureen Tracy
Canada Customs and Revenue Agency

Gerry Van Kessel
Intergovernmental Consultations on Asylum, Refugee and Migration Policies

Sandi Villeneuve
Association of International Customs and Border Agencies

Diane Vincent
Citizenship and Immigration Canada

Venita Warren
Citizenship and Immigration Canada (Youth Network)

Robert Whitelaw
Canadian Council of Better Business Bureaus

Randy Williams
Tourism Industry Association of Canada

Patricia Woroch
Immigration Services Society

Lynne Yelich
M.P., Blackstrap

Dr. Elia Zureik
Queen's University

ANNEX IV: TABLE DISCUSSION AND DIALOGUE

At the conclusion of the session, participants were given approximately forty-five minutes to discuss several key issues at their tables. This section seeks to capture both the oral reports to the plenary session at the end of the table discussions and the comments recorded in work books at each of the tables.

***Issue 1**: It is generally agreed that privacy is a fundamental concern when considering changes to improve the integrity of our documents. If biometric features were adopted as part of measures to improve document integrity,*

- ***What kinds of safeguards need to be put in place to ensure adequate privacy protection?***
- ***Do existing privacy safeguards (legislation, policy, institutions) provide a sufficient basis for dealing with the introduction of biometric identifiers?***
- ***What role does technology play in ensuring appropriate checks and balances?***

In response to the first question, the safeguards that participants identified included:

- The limitation of scope creep,
- Appropriate protection of biometric data,
- An independent oversight function based on statute, and
- Clarity and transparency around the systems purposes and processes.

On the question of existing privacy safeguards they felt that:

- Currently, there are not enough safeguards to prevent unauthorized use by the private sectors.
- There needs to be a better accountability framework.

Finally, participants felt that technology could play many roles. It could provide:

- Audit capability, and
- Counterfeit and tamper resistance that is appropriate to particular functions.

***Issue 2:** Document with biometric features can be implemented in programs with either voluntary or mandatory enrollment. If the goal of document integrity is to produce better, more secure documents that are less susceptible to counterfeiting and ID theft, many suggest that mandatory enrollment is required. On the other hand, privacy concerns suggest that individuals need to have a choice of whether or not their biometric is on a documnt or in a database. What do you think?*

Participants felt that there are important privacy implications to a national identity card whether or not it is mandatory. They felt that a business case should be made for the implementation of a national identity card, based on cost-benefit comparison versus document integrity solutions. There also has to be more discussion of the fundamental purpose of the card.

Some participants felt that this question was premature given that the government has not decided what the card will be used for. There was also concern about the eventual contracting out of card functions and the potential challenges this would create. Finally, there was concern that the uses for a national identity card would creep into unintended areas.

Issue 3: *In the current international security and law enforcement environment there is concern about document integrity in the context of travel and international movement of people. A number of jurisdictions (including most of Canada's major trading partners – USAs, EU, etc.) and international organizations are taking steps to introduce biometric features into travel documentation over the next two or three years:*

- ***What should Canada's response be to these developments?***
- ***How much scope does Canada have to act independently in this sphere?***

Some participants asked why we are leaping to the use of biometrics as a solution to a question that is not well understood. They asked whether Canada has ruled out other approaches such as the development of secure credentials in place of a national identity card. Others saw the need to develop such a card, in order to keep pace with our major trading partners. Initiatives that they suggested could be explored included: looking at travel documents, participating in standards bodies, and other activities to ensure that we are shaping the outcomes of international discussions on standards and priorities in a way that is acceptable to the collective values of Canadians. They stated that if Canada is to pursue such initiatives, then Canada should find like-minded partners with whom to work on developing effective international standards.

Other participants stated that there are a number of issues relating to the implementation of a national identity card that were not addressed at the Forum, including:

- The system of registration,
- Trade implications, both good and bad,
- Access to other landmasses besides North America,
- Sovereignty,
- Ethics and dignity,
- Revocation, and
- Is there a plan B for "when stuff happens," i.e., a worst case scenario?

ANNEX V: SUMMARY OF PUBLIC POLICY FORUM BACKGROUND PAPER

At the request of Citizenship and Immigration Canada, the Public Policy Forum prepared a background paper for the Biometrics Forum. This annex provides an overview of the paper. The full text of the the Background Paper and other documents relating to the Biometrics Forum are available on a Web site created by CIC for the event: **http://cic-forum.ca/english**.

Some of the key considerations with respect to the possible use of biometrics that were discussed in the paper included:

1) Applications

- *Identification versus verification*

2) Types of biometrics

- *Physiological characteristics versus behavioural characteristics*

3) Uses, including:

- *Storage on a computer chip*
- *Encryption on national identity cards*
- *Use in citizenship, immigration and travel contexts*

4) Performance Measurement

- *False rejection rate*
- *False acceptance rate*

The Background Paper also suggested a number of key questions for consideration in a public policy context:

1) Balancing security, privacy and civil liberties

- *What are the public values that should underpin decisions about the use of biometrics in citizenship and immigration identity documentation?*
- *Is the relationship among these values a zero-sum game? For example, is an increase in privacy protection necessarily at the expense of security (or vice-versa)?*

2) Purpose and Application

- *What public policy objectives will be served through the use of biometrics technologies in citizenship and immigration documentation?*
- *What applications (identification vs. verification) would be used?*

3) Privacy-enhancing technology and information management

- *Are technologies available that will ensure adequate protection of privacy and protection of personal information?*
- *What government databases would be linked to biometrics-enabled documentation? How would information be managed?*

4) Technological feasibility

- *Is the technology ready to meet expectations?*
- *Are there technologies, or combinations of technologies, that should be favoured? Ruled out?*

5) Biometrics and the law

- *Is the current legal framework adequate? What adjustments would be necessary?*
- *Is it enforceable?*

6) The governance dimension

- *Is a single national approach possible? Or, is this a matter best dealt with jurisdiction by jurisdiction and program by program?*
- *Are existing political and legal oversight and accountability mechanisms adequate? Or do new ones need to be created?*
- *How important is international harmonisation of design and execution?*

7) Financial and administrative capacity

- *Is a system of biometrics-enabled citizenship and immigration documentation financially and administratively feasible?*

8) Biometric-enabled cards – assembling the package

- *Putting all the elements together, what would a successful system of biometrics-enabled citizenship and immigration documentation look like?*
- *Should such a system of documentation be mandatory? If so, can it be implemented on a basis of voluntary compliance?*

The background paper prepared by the Public Policy Forum can be accessed at:

http://cic-forum.ca/english/background.pdf

For a hard copy, please contact the Public Policy Forum at:

Public Policy Forum
1405 – 130 Albert St.
Ottawa, Ontario K1P 5G4
Tel.: (613) 238-7160
Fax: (613) 238-7990

ANNEX VI: SUMMARY OF INSTANT POLLING

At the beginning and at the end of the second day of the Biometrics Forum, participants had the opportunity to provide instant feedback on a number of questions and issues, using technology from Sharpe Decisions Inc. This Annex presents the results of this instant polling.

First Session (morning of the second day of the Forum)

A) How important is it that the Government of Canada moves to enhance the integrity of its identity documents in the next two years?

1	Not important	3%
2	Important	27%
3	Very important	52%
4	I think there are more pressing priorities.	16%

B) Given your opinion regarding the importance of enhancing the integrity of identity documents, is your current preference to move towards:

1	A more comprehensive approach, like a national identity card.	35%
2	A more incremental approach, like strengthening existing documents like the passport or drivers licence.	48%
3	Maintaining the status quo, while improving foundation documents.	11%
4	I have no opinion.	4%

C) Coming here today, which of the following best characterizes your familiarity with biometrics?

1	Very poor	3%
2	Poor	25%
3	Good	50%
4	Very good	20%

D) Which of the following best describes your interests at this Forum?

1	I work directly with biometrics.	12%
2	I am interested in its various applications from a technological point of view.	9%
3	I am primarily interested in the social implications of biometrics.	62%
4	I am interested in other applications of biometrics.	10%
5	I am not at all interested in this technology.	0%
6	None of the above.	4%

E) How serious a problem do you think the fraudulent use of identity documents is in Canada?

1	Not at all serious	1%
2	Not very serious	3%
3	Moderately serious	21%
4	Somewhat serious	25%
5	Extremely serious	35%
6	Don't know - No reponse.	12%

F) Do you personally support or oppose the use of biometrics by the federal government as a way of reducing the fraudulent use of identity documents?

1	Strongly oppose	4%
2	Somewhat oppose	17%
3	Neither	4%
4	Somewhat support	28%
5	Strongly support	44%

G) Given the growing concerns about verifying the identity of individuals, how likely do you think it is that by the end of the decade, almost every Canadian adult will have at least one biometric ID on file to verify their identity?

1	Not at all likely	1%
2	Not very likely	1%
3	Somewhat likely	8%
4	Very likely	83%
5	Don't know	5%

Second Session (afternoon of the second day of the Forum)

H) Given the growing use of biometrics by both the public and private sectors, some people believe that governments should be dealing with regulatory issues related to the use, storage and sharing of this type of information. Which one of the following statements best reflects your views?

1	Governments should deal with the regulatory issues	55%
2	There are too many risks associated with biometrics	6%
3	More information on what this means needs to be communicated	38%

I) Which of the following statements best reflects your views?

1	Biometrics have the potential to reduce millions of dollars in lost revenues due to the use of fraudulent identity documents. We owe it to ourselves to take a serious look at this technology.	51%
2	Organized crime is very advanced, particularly elements involved in the manufacture and trafficking of illegal documents, it will only be a matter of time before they can circumvent this technology.	25%
3	Don't know - No reponse.	23%

J) Which of the following statements best reflects your views?

1	I could accept the use of biometrics in a Citizenship and Immigration context, if the government provided a solid case for how it would be protected from abuse and misuse.	72%
2	Given that there have been numerous examples of how governments have lost or mishandled secret personal information, no one should have to provide this type of personal information including newcomers to Canada.	12%
3	Don't know - No reponse.	15%

K) Which of the following statements best reflects your views?

1	Documents that are used to establish identity are lost or stolen every day. If biometric information fell into the wrong hands it would represent an even greater threat to individual privacy.	27%
2	Stealing an individual's identity has become increasingly easy. Using biometric technologies will make it harder for criminals to duplicate or misrepresent current identity documents and would actually improve the protection of personal information.	62%
3	Don't know - No response	9%

L) Which of the following statements best reflects your views?

1	It makes sense to implement biometrics but only for those who stand to benefit from the technology, such as passengers who provide an iris scan to move quickly through airport security.	9%
2	The security benefits of implementing biometrics would be lost if it were implemented on a voluntary basis.	15%
3	Other issues need to be considered before detailing with mandatory or voluntary enrollment.	74%

M) Which of the following statements best reflects your views?

1	Given global realities, all individuals wishing to come to Canada, either as a refugee or an immigrant, should provide biometric identifiers with their applications.	36%
2	It would be unfair to single out newcomers to Canada. The problems of fraudulent ID are more pervasive and require a more comprehensive response.	54%
3	Don't know - No response.	9%

N) How important is it that the Government of Canada move to enhance the integrity of its identity documents in the next two years?

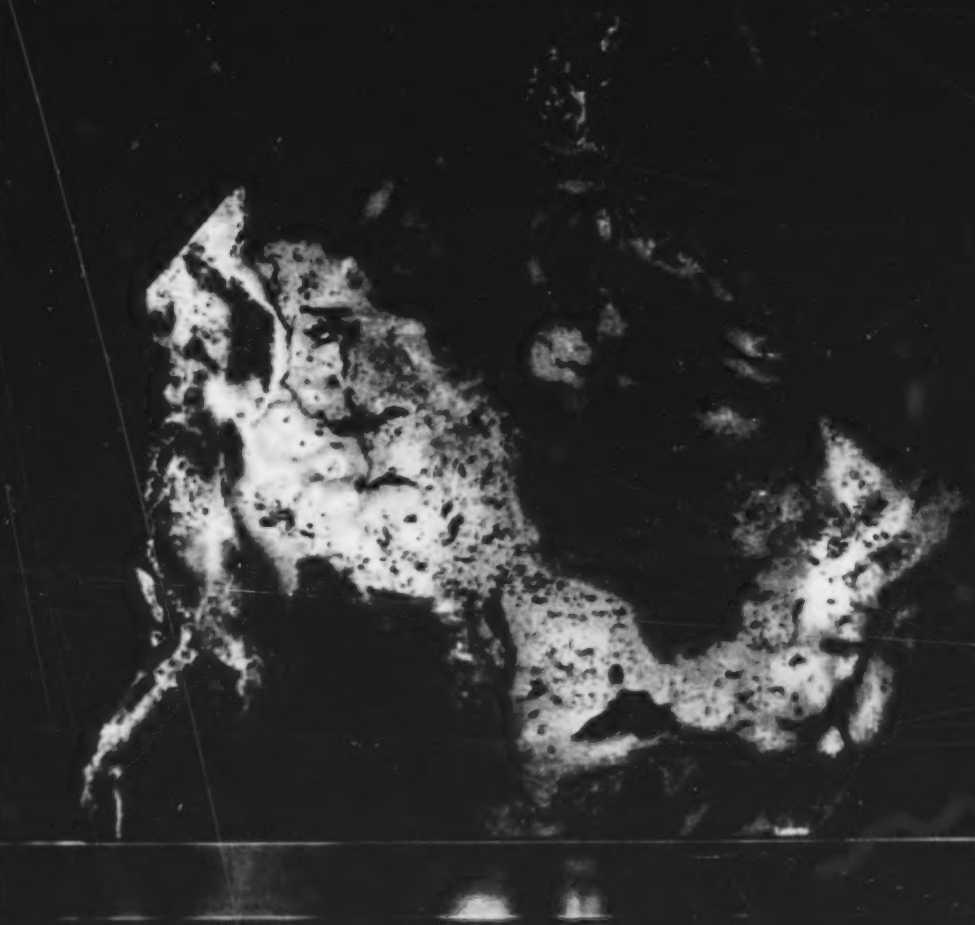
1	Not important	0%
2	Important	19%
3	Very important	61%
4	I think there are more pressing priorities.	19%

O) Given your opinion regarding the importance of enhancing the integrity of identity documents, is your current preference to move toward :

1	A more comprehensive approach, like a national identity card.	23%
2	A more incremental approach, like strengthening existing documents – such as the passport or driver's licence.	56%
3	Maintaining the status quo, while improving foundation documents.	20%
4	I have no opinion.	0%

La biométrie

Incidences et applications pour la citoyenneté et l'immigration



Actes d'un forum tenu par
Citoyenneté et Immigration Canada

Le 7 et 8 octobre 2003 – Ottawa (Ontario)

Public Policy Forum
Forum des politiques publiques

La biométrie :

Incidences et applications pour la citoyenneté et l'immigration

Actes d'un forum tenu par Citoyenneté et Immigration Canada

Les 7 et 8 octobre 2003 – Ottawa (Ontario)

Préparé par le Forum des politiques publiques pour

Citoyenneté et Immigration Canada

À PROPOS DU FORUM DES POLITIQUES PUBLIQUES

Recherche de l'excellence au gouvernement

Le Forum des politiques publiques est un organisme indépendant sans but lucratif qui vise à améliorer la qualité de l'administration au Canada en suscitant un meilleur dialogue entre les secteurs public, privé et bénévole. Les membres du Forum, qui sont issus du monde des affaires, des gouvernements fédéral et provinciaux, des organismes bénévoles et du mouvement ouvrier, partagent l'idée qu'une fonction publique efficace et efficiente est un atout majeur pour notre qualité de vie et pour notre position concurrentielle à l'échelle mondiale.

Depuis sa fondation en 1987, le Forum des politiques publiques s'est taillé une réputation de facilitateur neutre et digne de confiance, capable de réunir toute une gamme d'intervenants en vue d'un dialogue constructif. Son programme de recherche fournit des renseignements objectifs à l'appui de la prise de décision collective. En favorisant un plus grand échange d'information et des liens plus étroits entre les gouvernements et les autres secteurs, le Forum des politiques publiques veille à ce que le Canada prenne des orientations plus dynamiques, mieux coordonnées et mieux adaptées aux défis et possibilités de l'avenir.

À PROPOS DES AUTEURS

David Brown est directeur des Projets spéciaux au Forum des politiques publiques.

David Brook est un associé du Forum des politiques publiques.

Nous voudrions remercier les membres du Groupe de travail de Citoyenneté et Immigration Canada sur l'intégrité des documents, et plus particulièrement Peggi McNeil, directrice, et Milena Isakovic, assistante de recherche au Forum des politiques publiques, pour leur précieux concours.

Le Forum des politiques publiques
1405-130, rue Albert
Ottawa (Ontario) K1P 5G4

Tél.: (613) 238-7160
Fax: (613) 238-7990

www.ppforum.ca

TABLE DES MATIÈRES

INTRODUCTION 1

ANNEXE I : RÉSUMÉ DE CHACUN DES EXPOSÉS 9

DISCOURS D'OUVERTURE : TROUVER UN JUSTE ÉQUILIBRE ENTRE LA SÉCURITÉ ET LES LIBERTÉS PUBLIQUES – Pr Alan Dershowitz 9

DISCOURS D'OUVERTURE – L'honorable Denis Coderre 12

CONFÉRENCIER D'HONNEUR : BIOMÉTRIE – PASSÉ, PRÉSENT ET AVENIR – Colin Soutar, Ph. D. 15

PREMIÈRE RÉUNION D'EXPERTS – LA BIOMÉTRIE DANS LE CONTEXTE INTERNATIONAL 18

Martin Giles, directeur adjoint, Service d'immigration du Royaume-Uni, Home Office 18

Gillian Russell, Direction générale, Justice et affaires intérieures, Commission européenne 20

W. Russell Neuman, Ph. D., analyste principal des politiques, Bureau de la politique scientifique et technologique de la Maison-Blanche 21

Gerry Van Kessel, coordonnateur, Consultations intergouvernementales sur les politiques d'asile, de reconnaissance du statut de réfugié et de migration en Europe, en Amérique du Nord et en Australie 23

CONFÉRENCIER INVITÉ AU DÉJEUNER – Frank Graves 26

CONFÉRENCIÈRE DE L'APRÈS-MIDI : QUESTIONS LIÉES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS – Stephanie Perrin 29

DEUXIÈME RÉUNION D'EXPERTS : BIOMÉTRIE – COMPRENDRE ET ÉVALUER LES INCIDENCES DE LA BIOMÉTRIE 32

Roger Gibbins, président-directeur général, Canada West Foundation 32

Jennifer Stoddart, présidente, Commission d'accès à l'information du Québec 34

Raj Nanavati, International Biometrics Group 37

Raymonde Folco, députée de Laval-Ouest 40

CONCLUSIONS ET ORIENTATIONS CONCERNANT LES ÉVENTUELLES MESURES À PRENDRE – L'honorable Denis Coderre 41

INTRODUCTION

Les préoccupations récentes en matière de sécurité internationale, les initiatives concernant la frontière, et la fréquence plus élevée de l'usurpation d'identité et de la fraude touchant celle-ci font ressortir la nécessité de mieux protéger l'intégrité des documents canadiens d'identité, d'immigration, de citoyenneté et de voyage. La biométrie se présente comme une technologie puissante, mais controversée, pouvant peut-être aider à relever ces défis des politiques publiques. Dans ce contexte, le ministre de la Citoyenneté et de l'Immigration, l'honorable Denis Coderre, a encouragé la tenue d'un débat public sur la question de l'élaboration d'une politique d'identité nationale et sur la possibilité d'utiliser la technologie biométrique dans les documents d'identité.

Au cours des dernières années, le Comité permanent de la citoyenneté et de l'immigration a tenu des audiences sur les avantages et les inconvénients reliés à une éventuelle carte d'identité nationale. À l'issue de consultations poussées, il a produit un rapport provisoire dans lequel il affirmait que la question exigeait un examen plus approfondi, y compris un débat avec la population canadienne, avant que des recommandations définitives ne puissent être formulées. Cette question et d'autres de même nature font aussi l'objet de pourparlers entre les gouvernements fédéral, provinciaux et territoriaux.

Les 7 et 8 octobre 2003, dans un effort pour promouvoir le dialogue sur cette question, Citoyenneté et Immigration Canada (CIC) a tenu un forum sur la biométrie à Ottawa, pour étudier l'utilisation de la technologie biométrique dans le contexte des mesures destinées à mieux protéger l'intégrité des documents d'identité et de voyage pour les citoyens canadiens et les résidents permanents du Canada (Annexe II : Ordre du jour).

Le forum visait les objectifs suivants :

- explorer la biométrie comme une technologie puissante susceptible de faciliter l'atteinte de futurs objectifs stratégiques importants;
- améliorer et élargir le débat actuel sur les aspects techniques et sociaux reliés à l'utilisation de la biométrie à l'appui de l'intégrité des documents et de la vérification de l'identité;
- comparer les avantages et les inconvénients d'une approche globale de la « carte d'identité nationale » par rapport à une stratégie plus progressive qui consisterait à améliorer les nombreux documents d'identité existants;
- engager un dialogue sur les questions importantes avant la mise en œuvre de toute politique.

Articulé autour d'un ensemble de conférenciers invités, de groupes d'experts, de discussions de groupe et de séance de rétroaction, le forum visait à sensibiliser la population et à explorer les applications et les incidences possibles de la biométrie dans le contexte de la citoyenneté et de l'immigration. L'événement a réuni des intervenants nationaux et des experts internationaux des divers secteurs concernés pour tenir un dialogue équilibré; ce dernier visait à informer et à promouvoir la réflexion sur la politique du Ministère relativement aux questions essentielles reliées à l'utilisation des technologies biométriques destinées à renforcer l'intégrité des documents (Annexe III : Participants inscrits).

Pour l'occasion, le Forum des politiques publiques a préparé un document d'information pour alimenter la réflexion sur la politique de CIC et pour donner aux participants du Forum et à la population canadienne un

aperçu général des grands enjeux de la biométrie dans le contexte de la citoyenneté et de l'immigration[1]. Le document a été préparé à la demande de CIC et s'appuie sur des travaux de recherche et des entrevues d'experts clés (pour un court résumé du document d'information, veuillez vous reporter à l'annexe V).

Au cours de la rencontre d'une journée et demie, les participants et les conférenciers ont entrepris un dialogue sur un grand nombre des questions abordées dans le document d'information. Le présent rapport tente de présenter les grands enjeux, les difficultés, les orientations et les questions abordés au cours de ce forum. Il débute par un aperçu des questions clés abordées au cours du forum et, en particulier, des thèmes et des consensus qui s'en sont dégagés. L'annexe I résume le contenu des exposés et des réunions d'experts ainsi que les questions posées par les participants et les discussions qui ont suivi. On peut trouver le texte intégral ou un résumé de la plupart des exposés dans le site Web du Forum sur la biométrie à : **http://cic-forum.ca**.

À la fin de la deuxième journée, on a demandé aux participants, qui étaient réunis en groupes de six à chacune des tables, de discuter de l'un des trois sujets ayant trait à l'utilisation de la biométrie et d'une éventuelle carte d'identité nationale. Chaque groupe devait consigner les points de vue exprimés, et ces derniers sont résumés à l'annexe IV. En outre, à deux reprises au cours de la deuxième journée, les participants ont été priés d'enregistrer leur point de vue par vote électronique, ce qui a permis d'obtenir des résultats instantanés. Les résultats de ces « sondages instantanés » figurent à l'annexe VI.

Actes et conclusions du forum

Le forum de Citoyenneté et Immigration sur la biométrie a réuni un grand nombre de participants et de conférenciers issus de milieux fort variés (veuillez vous reporter à l'annexe III pour la liste complète des participants et des conférenciers). Les participants ont été choisis de manière à apporter le plus grand nombre possible de points de vue, de positions et d'opinions sur l'identité, le respect de la vie privée et d'autres questions connexes. Cette diversité de participants a permis un dialogue et un débat dynamiques tout au long de la journée et demie qu'a duré le forum, sur de nombreux sujets importants, notamment sur l'utilisation des documents d'identité dotés de caractéristiques biométriques dans le contexte de la citoyenneté et de l'immigration.

Le forum s'est ouvert avec le discours prononcé au dîner d'ouverture par le P[r] Alan Dershowitz, professeur de droit Felix Frankfurter de l'Université Harvard (veuillez vous reporter à l'annexe I, pp. 9-12); ce dernier a abordé quelques-uns des problèmes qui, à son avis, sont reliés à la carte d'identité nationale et à l'utilisation de la biométrie. Selon lui, il faut distinguer deux grandes catégories de problèmes : ceux qui ont trait à la carte d'identité elle-même et ceux qui concernent son utilisation. Le P[r] Dershowitz a insisté sur l'importance de tenir, dès à présent, un débat sur l'utilisation de la biométrie, afin que la politique soit le moteur du développement de la technologie et non l'inverse. Il a aussi fait valoir l'importance de ne pas compter sur l'échec de la technologie pour protéger la vie privée, mais plutôt de résoudre les problèmes ayant trait à la vie privée dès le début du développement et de l'application de toute nouvelle technologie, y compris d'une carte d'identité dotée de caractéristiques biométriques.

La séance du matin a débuté avec une introduction présentée par l'honorable Denis Coderre, ministre de la Citoyenneté et de l'Immigration, qui a souligné l'importance du forum et l'urgence de résoudre les questions d'identité et de l'utilisation de la biométrie (annexe I : pp. 13-16). Selon le Ministre, malgré les nombreuses et importantes difficultés à résoudre en rapport avec l'utilisation de la biométrie, les

1 Le Document d'information et d'autres documents ayant trait au Forum sur la biométrie se trouvent dans le site Web créé par CIC pour l'occasion : **http://cic-forum.ca/francais**.

technologies biométriques sont ici pour rester. Comme tel, selon lui, le statu quo est inacceptable et il est important que tous les Canadiens discutent de la meilleure façon de protéger l'intégrité des documents pour prévenir la fraude reliée à l'identité tout en respectant les droits des individus.

Plus tard dans la matinée, M. Colin Soutar, Conseiller technique principal à l'Association canadienne de technologie de pointe, une sommité des technologies biométriques, a traité de certains aspects concernant la mise en service d'une carte d'identité dotée de caractéristiques biométriques, notamment de la différence entre vérification et identification (annexe I : pp. 17-20). À son avis, il est effectivement possible d'améliorer la sécurité tout en protégeant l'identité, mais cela exige que nous établissions les bonnes priorités en matière de politique et que nous développions des technologies capables de répondre à ces besoins.

Le reste de la matinée a été consacré à un groupe d'experts internationaux qui ont discuté du rôle et de l'application des technologies biométriques dans leurs contextes respectifs (pour la liste complète des membres des groupes d'experts, veuillez consulter l'Annexe II : Ordre du jour. Les notes sur le groupe d'experts se trouvent à l'annexe I, pp. 21-30.) Les panélistes ont discuté du rôle des systèmes biométriques en immigration dans les pays de l'Union européenne, avec le système Eurodac, et au Royaume-Uni. Ils se sont également penchés sur l'importance des technologies biométriques pour le programme de sécurité américain et sur la possibilité d'utiliser les technologies biométriques dans le contexte de l'immigration et des mouvements de réfugiés au Canada.

Au cours de la période de questions qui a suivi la réunion d'experts internationaux, les participants ont dit craindre l'émergence d'une mentalité du « nous contre eux » si l'on impose la biométrie dans le cadre de l'immigration. Les panélistes ont répondu que les utilisateurs légitimes du système d'immigration sont généralement en faveur d'une carte unique dont l'intégrité serait hautement protégée et qui leur donnerait accès le plus facilement possible aux services dont ils ont besoin. D'autres participants se sont inquiétés de la possibilité d'abus que présente un système biométrique. Les panélistes ont alors affirmé que tout système peut faire l'objet d'abus si on utilise une approche inadéquate ou irresponsable. En réalité, la biométrie doit absolument faire l'objet d'un débat ouvert et transparent, peu importe l'utilisation qu'on veut en faire.

Le conférencier invité au déjeuner était Frank Graves, président, Les Associés de recherche EKOS Inc., qui a présenté des chiffres récents sur les opinions des Canadiens (annexe I : pp. 31-34). Selon M. Graves, une nette majorité de Canadiens seraient prêts à appuyer l'introduction d'une carte d'identité nationale si on leur donnait un argument de taille pour le faire; mais les Canadiens ne voient pas la nécessité de choisir entre la sécurité et la protection de la vie privée. Pour M. Graves, les Canadiens vont exiger un haut niveau de ces deux éléments et ils ne sont pas prêts à mettre en péril ni l'un ni l'autre.

L'après-midi a débuté par un exposé de Stéphanie Perrin, de Discrétion digitale, sur les problèmes de protection de la vie privée entourant l'utilisation de la biométrie et l'introduction d'une carte d'identité nationale (annexe I : pp. 35-38). Mme Perrin s'est interrogée sur la nécessité d'apporter des solutions biométriques aux problèmes liés à l'identité, sur l'importance d'une surveillance indépendante des applications biométriques et sur l'obligation de poursuivre la recherche sur les répercussions à long terme de la mise en œuvre de toute forme de carte d'identité nationale.

Le groupe d'experts de l'après-midi s'est surtout attaché à comprendre et à évaluer les répercussions des technologies biométriques sur la vie privée dans le contexte canadien (pour la liste complète des panélistes, veuillez vous reporter à l'Annexe II : Ordre du jour. Les notes sur le groupe d'experts et sur les discussions qui ont suivi se trouvent à l'annexe I, pp. 39-49). Les panélistes ont soulevé plusieurs questions sur le but, les utilisations et la nature d'une carte d'identité nationale. Ils ont aussi examiné l'importance d'une législation en matière de protection de la vie privée, la nécessité d'une surveillance indépendante des systèmes biométriques et des données recueillies à l'aide de ces derniers et la nécessité

d'envisager d'autres solutions, par exemple, d'améliorer l'intégrité des documents de base (tels que les certificats de naissance). Finalement, l'un des panélistes a avancé un argument en faveur d'une approche fondée sur les principes pour utiliser la biométrie.

Au cours des échanges qui ont suivi, les participants et les panélistes ont insisté sur la nécessité d'assurer une mise en service adéquate des technologies biométriques, sur l'importance d'une surveillance et d'une vérification indépendantes et sur l'obligation pour le gouvernement de présenter une justification convaincante avant d'introduire la carte d'identité nationale.

Pour terminer, les participants ont discuté, à leurs tables respectives, de trois aspects de la biométrie et ils ont ensuite présenté leurs comptes rendus en séance plénière. Les points soulevés au cours de ces délibérations sont résumés à l'annexe IV. Le ministre Coderre a clos le forum par une courte allocution dans laquelle il réitérait sa ferme conviction que les technologies biométriques sont une réalité bien implantée et qu'elles sont essentielles pour tous les Canadiens (annexe I : pp. 50-51). Comme tel, il a dit souhaiter informer tous les Canadiens sur cette question et encourager les discussions dans tous les salons de la nation.

Bien qu'aucun consensus n'ait été atteint au cours du forum, certains aspects ont rallié les opinions à l'appui de la décision d'aller de l'avant. Les points clés suivants ont été établis :

L'utilisation de la biométrie en vue de documenter l'identité pose de véritables problèmes qui doivent faire l'objet d'un débat public sérieux.

- Les questions ayant trait aux documents d'identité ont une incidence directe sur tous les Canadiens. En revanche, la population est peu informée de ces questions et des choix qu'elles imposent, et ses opinions reposent souvent sur des impressions.
- Il existe actuellement un vide politique et législatif dans ce secteur de la politique publique en pleine évolution.
- Le Canada a une expérience considérable en ce domaine, tant sur le plan technologique qu'en ce qui concerne les aspects étroitement reliés de la protection de la vie privée et de la gestion des données. L'expérience sur la scène internationale est, elle aussi, pertinente, à la fois pour proposer les meilleures pratiques et à cause du caractère interdépendant de secteurs de politique publique tels que l'immigration.
- De l'avis généralisé des experts, ce domaine fait appel à une multiplicité de disciplines et de champs de compétence

Le statu quo n'est pas viable.

- Les Canadiens ne peuvent pas compter sur l'échec de la technologie pour protéger leur vie privée.
- Les technologies biométriques sont maintenant appliquées, et leur utilisation ira en augmentant. Par conséquent, il est important d'entreprendre un débat public ouvert et exhaustif sur le but de ces technologies, leur utilisation et les mesures de protection qu'il convient de mettre en place pour éviter d'éventuels abus.
- Il faut s'assurer que les impératifs stratégiques dictent le développement de la technologie et non l'inverse.

La dichotomie perçue entre la sécurité et la protection de la vie privée est fausse.

- À la fin du forum, un grand nombre de participants et de conférenciers, sinon la majorité, ont convenu que, malgré les difficultés que présente l'utilisation de la biométrie dans certains contextes, la biométrie ne comporte en soi aucun élément qui améliore ou qui limite le respect de la vie privée. La biométrie doit donc être examinée dans le cadre d'applications précises et de leur contexte de gestion des données

Il faut procéder à une étude de rentabilisation pour les applications biométriques dans les documents d'identité, y compris pour la carte d'identité nationale

- Les participants ont convenu qu'il était absolument nécessaire de déterminer quels problèmes seraient résolus par les instruments biométriques dans les documents d'identité et quelles difficultés d'ordre public une carte d'identité nationale unique dotée de caractéristiques biométriques seraient aplanies.
- On pourrait ensuite mieux cerner les fonctions, les buts, les utilisations et les garanties qu'il faudrait établir avant d'introduire une telle carte.
- Ce n'est qu'une fois ce travail terminé que l'on pourrait établir une comparaison entre les coûts et les avantages d'une carte d'identité nationale et d'autres solutions de protection de l'intégrité des documents.
- De nombreux participants étaient préoccupés par les coûts qu'entrainerait la carte d'identité nationale, notamment pour la mise en œuvre d'un système efficace d'inscription et pour les mécanismes administratifs qu'il faudrait mettre en place pour le rendre fonctionnel sur une base quotidienne. Aucun chiffre définitif n'a été avancé pour le coût d'une telle entreprise (les estimations allaient de 340 millions de dollars à plus de 5 milliards de dollars), mais les participants étaient généralement d'avis qu'avant d'envisager l'adoption de cette carte, il faudrait absolument entreprendre une analyse approfondie des coûts par rapport aux avantages

La biométrie a été appliquée avec succès dans d'autres pays

- Les exposés présentés tout au long de la journée donnent à penser que les identificateurs biométriques ont été utilisés avec succès dans d'autres pays, pour répondre à des besoins clairement établis, par exemple, en ce qui a trait à l'immigration.
- Voici quelques points retenus des exemples de l'étranger :
    - o L'importance d'élaborer et de mettre en œuvre des programmes faisant appel à des instruments biométriques en s'appuyant sur une politique bien conçue et sur une saine gestion.
    - o L'importance de bien comprendre les applications particulières pour lesquelles les technologies biométriques seront utilisées.
    - o Les garanties de protection de la vie privée, pour être efficaces, doivent être intégrées dans le système dès le début.
    - o Tout système technologique qui présente un danger d'atteinte à la vie privée de tout individu ou groupe doit faire l'objet d'une surveillance indépendante efficace.

Il faudrait résoudre un certain nombre de problèmes techniques avant d'introduire une carte d'identité nationale dotée de caractéristiques biométriques.

- Les participants ont déterminé un certain nombre de problèmes techniques et de considérations dont il faudrait tenir compte dans l'élaboration et la mise en service d'une carte biométrique, notamment :
    - La carte servira-t-elle principalement à la vérification ou à la confirmation de l'identité?
    - Veiller à ce que les fonctions biométriques et les données qui en découlent soient gérées correctement.
    - La méthode de saisie et de traitement des données biométriques (utilisation d'une image ou d'un modèle).
    - Le type d'instrument biométrique à utiliser compte tenu de l'équilibre très différent des considérations qui s'applique à chaque cas.

La carte d'identité nationale, si elle est introduite, devrait être obligatoire et non facultative

- Des arguments ont été présentés en faveur de l'approche facultative aussi bien qu'en faveur de l'approche obligatoire; cependant, dans l'ensemble, les participants ont penché en faveur d'une carte obligatoire, en supposant que l'on adopte une carte d'identité nationale. Les arguments étaient les suivants :
    - Certains groupes n'auraient peut-être pas les moyens d'obtenir une carte facultative ou n'y auraient peut-être pas accès.
    - On doit s'assurer que toute atteinte aux libertés fondamentales est équitablement répartie dans toute la population, pour assurer un débat public ouvert et équilibré.
    - Par ailleurs, plusieurs participants ont mis en garde contre la « reptation de fonction » qui accompagne toute carte nationale ou universelle.

La résolution satisfaisante des questions de respect de la vie privée et de protection des renseignements personnels doit faire partie intégrante de la conception et de l'élaboration de tout document doté de caractéristiques biométriques

- Les participants ont exprimé leurs craintes quant à un certain nombre de questions de respect de la vie privée :
    - Accès non autorisé à l'information – les participants s'inquiètent de la possibilité, pour des organismes ou agents gouvernementaux non autorisés ou pour le secteur privé, d'avoir accès à des renseignements recueillis à l'aide d'instruments biométriques. Il y a aussi la question – étroitement liée – de savoir si, et selon quelles modalités, les données seront réutilisées ou communiquées à d'autres.
    - Risque de reptation de fonction – selon de nombreux participants, peu importe la carte et malgré les fins pour lesquelles elle a été conçue, les données qu'elle contient finiront par servir à d'autres fins que celles prévues. Certains craignent en particulier l'élargissement des fonctions d'une carte délivrée par le gouvernement jusqu'à donner accès aux services gouvernementaux ou même à servir aux transactions commerciales (comme c'est déjà le cas dans d'autres pays).

- Principes de confidentialité – en revanche, les participants conviennent que les principes de confidentialité et de gestion des données acceptés à l'échelle nationale et internationale offrent une base solide pour réglementer l'utilisation de la biométrie, et que des modèles législatifs utiles existent déjà au Canada.

En définitive, les participants sont d'avis qu'il nous faut une solution « typiquement canadienne » au problème des documents d'identité. D'un autre côté, ils reconnaissent que la pression exercée par la communauté internationale en vue de mettre en œuvre une forme quelconque d'application biométrique, qu'elle se limite aux documents de voyage ou qu'elle soit plus étendue, ne fera que s'intensifier au cours des prochaines années. Comme tel, il semble que le gouvernement fédéral soit entièrement fondé à mettre en œuvre une politique et une stratégie en matière de documents d'identité, notamment à l'aide de la biométrie, dans son propre champ de compétence, et à collaborer avec les provinces et les territoires en vue d'élaborer une approche nationale à cet égard. Il devrait aussi continuer à participer à des débats internationaux sur ces questions.

ANNEXE I : RÉSUMÉ DE CHACUN DES EXPOSÉS

Discours d'ouverture : Trouver un juste équilibre entre la sécurité et les libertés publiques – Alan Dershowitz
Professeur de droit Felix Frankfurter
Harvard Law School

Le Pr Dershowitz a commencé son discours en répartissant les différents problèmes de l'élaboration et de la mise en œuvre d'une carte d'identité nationale en deux groupes :

- ceux qui ont trait à la carte d'identité nationale elle-même;
- ceux qui ont trait à son utilisation dans un contexte particulier.

Le premier groupe de problèmes (ceux qui ont trait à la carte d'identité nationale elle-même) est le suivant :

1) Quel type de carte devrait-on utiliser?

- Une carte minimaliste qui pourrait n'indiquer que le nom et le pays de citoyenneté de l'individu ou une carte maximaliste qui pourrait comporter toutes les données d'identification de l'individu, y compris son casier judiciaire, le cas échéant? La carte serait-elle dotée d'un identificateur biométrique?

2) Dans quelles circonstances le gouvernement devrait-il avoir le pouvoir d'exiger une pièce d'identité

- Quand un citoyen devrait-il avoir le droit de refuser de s'identifier? On pourrait certainement avancer que le « sentiment de liberté » serait perdu si un agent de police pouvait demander à une personne de montrer ses papiers d'identité en tout temps, peu importe la raison? D'un autre côté, le « sentiment de sécurité » pourrait être compromis si personne ne pouvait être forcé à montrer ses papiers d'identité.

3) Comment peut-on être certain que l'information qui figure sur la carte correspond à son détenteur

- Pour le Pr Dershowitz, cela soulève deux problèmes : la personne qui présente une carte est-elle celle dont il est question sur la carte, et la personne sur la carte est-elle vraiment qui elle prétend être? À son avis, le premier problème, en particulier, peut être résolu grâce à un identificateur biométrique. Quant au deuxième, il requiert de bonnes vérifications des antécédents.

4) La carte devrait-elle être obligatoire ou facultative

- Le Pr Dershowitz a soulevé un certain nombre de questions concernant le caractère obligatoire ou facultatif de la carte d'identité nationale. Pour lancer le débat, il a donné l'exemple d'un programme de présélection des voyageurs à faible risque qui permet au voyageur de passer plus rapidement les contrôles à l'aéroport s'il répond à un ensemble de critères particuliers. La preuve d'inscription à un tel programme pourrait reposer sur un identificateur biométrique. Le Pr Dershowitz affirme qu'une telle application serait probablement acceptable pour la majorité des individus, si le fait de ne pas être inscrit au programme avait pour seule conséquence d'allonger quelque peu le temps passé dans les files d'attente. Cependant, si la personne inscrite demeure dans la file d'attente pendant quelques minutes alors que la personne non inscrite doit attendre pendant des heures, s'agit-il vraiment d'un choix? Le Pr Dershowitz soulève d'autres questions :
    - o Si la carte est obligatoire, tous doivent-ils la porter sur eux en tout temps?
    - o Y aurait-il un délai de grâce pour produire la carte lorsqu'on nous la demande?

5) La carte d'identité devrait-elle avoir une portée locale, nationale ou internationale?

- Pour le Pr Dershowitz, chacun de ces scénarios comporte des avantages et des inconvénients, mais en ce moment, les normes internationales (comme pour les permis de conduire) ne sont pas beaucoup utilisées. Aux États-Unis, on a tenté d'instaurer un permis de conduire national, mais de nombreux groupes conservateurs s'y sont opposés, certains allant jusqu'à rejeter l'idée d'un format uniforme dans tous les États.

Le deuxième groupe de problèmes présenté par le Pr Dershowitz concerne l'application en tant que telle d'une carte d'identité nationale dans un contexte réel :

1) À quelle sorte de base de données la carte serait-elle reliée?

- Pour le Pr Dershowitz, les points suivants sont importants :
    - o Quels renseignements la base de données devrait-elle contenir ?
    - o La carte serait-elle reliée à une seule base de données ou à plusieurs?
    - o Des données seraient-elles échangées avec d'autres bases de données?

2) Le secteur privé devrait-il avoir accès à cette information

- Selon le Pr Dershowitz, l'accès aux différentes bases de données à partir d'une seule carte ne devrait pas poser de problème, en autant que le coupe-feu entre les bases de données est suffisamment sûr.

3) Est-il possible d'appliquer à l'information contenue dans une carte d'identité nationale le principe de l'accès sélectif

- Le Pr Dershowitz est d'avis que, théoriquement, il est possible de limiter l'accès à cette information. Il a donné l'exemple de la carte d'identité malaisienne qui, jusqu'à ces derniers mois, renfermait beaucoup plus d'information, à son avis, que tout citoyen canadien ou américain ne permettrait à son gouvernement de réunir en un seul lieu. Si la carte malaisienne a été acceptée, c'est que le gouvernement a donné l'assurance qu'aucun organisme gouvernemental ne pourrait accéder à toute l'information contenue dans la carte, cette information étant séparée par des coupe-feu et accessible uniquement de façon sélective.

Le Pr Dershowitz a poursuivi son allocution en soulignant l'importance de tenir un débat pour déterminer quelles sortes de technologies sont appropriées et dans quelles circonstances il convient de les appliquer, et ce, avant qu'elles ne fassent leur entrée sur le marché, afin que les considérations stratégiques dictent le développement de ces technologies et non l'inverse. Il a réitéré cette opinion en ajoutant qu'on ne peut rester insensible aux abus qui découlent de la centralisation des pouvoirs. Il faut absolument tenir un débat pour déterminer quelles sortes de renseignements les gouvernements peuvent recueillir et conserver dans des bases de données.

Après ces propos sur la carte d'identité nationale, le Pr Dershowitz a examiné plus en profondeur les moyens par lesquels cette carte pourrait être mise en œuvre. À son avis, une carte d'identité nationale pourrait fonctionner de plusieurs façons différentes – une fois insérée dans une machine, la carte pourrait donner un résultat d'identification négatif ou positif, ou encore générer une quantité énorme d'informations tirées d'une base de données centrale. L'une ou l'autre de ces fonctions pourrait être utilisée pour toutes sortes d'applications. Le Pr Dershowitz s'est ensuite penché sur les préoccupations exprimées par certains défenseurs de la protection de la vie privée et par d'autres participants, qui craignent un éventuel « glissement », c'est-à-dire l'utilisation de cartes d'identité à des fins autres que celles pour lesquelles elles ont été prévues et qui constituent une intrusion plus poussée dans la vie privée. Il a affirmé que la seule chose plus dangereuse qu'un glissement est un « glissement imperceptible » : toute carte, biométrique ou autre, qui offre une amélioration sur les méthodes existantes de vérification de l'identité finira sans aucun doute par servir à des fins tout à fait autres. En réalité, a-t-il soutenu, il vaut mieux tenir un débat ouvert et public au sujet des utilisations possibles d'un tel dispositif, plutôt que de laisser ce dernier servir à d'autres fins, sans que nous ayons tenu préalablement un débat ou un examen approfondi.

Un des arguments en faveur de l'adoption d'une carte d'identité nationale minimaliste présenté par le Pr Dershowitz est qu'elle permet de réduire le besoin ou d'éliminer en grande partie la justification du profilage de l'origine ethnique ou nationale. Selon lui, si un pays doit restreindre les droits de ses occupants, il vaut mieux qu'il les restreigne pour l'ensemble de la population que de viser de petits groupes (comme les Américains musulmans, à la suite des attentats du 11 septembre 2001). Si la liberté de l'ensemble de la population est limitée, les conséquences seront les mêmes pour tout le monde et il est fort probable que cela suscitera un débat approfondi et animé sur la question.

Le Pr Dershowitz a ensuite soulevé la question de l'utilisation d'appareils de reconnaissance faciale dans les endroits publics. Bien que ces appareils ne fonctionnent pas encore assez bien pour être implantés (ils donnent beaucoup trop de faux positifs et les échecs à la reconnaissance sont trop nombreux pour qu'ils soient efficaces), ils seront bientôt conformes à des normes raisonnables. Selon lui, la société doit commencer dès aujourd'hui à débattre des questions relatives à l'utilisation de ces technologies, car autrement, lorsque la technologie sera au point et en place, il sera trop tard pour le faire.

Un des thèmes clés abordés par le Pr Dershowitz est que selon lui, les tenants des libertés fondamentales commettent une grave erreur en se fiant à l'inefficacité de la technologie pour défendre la protection des renseignements personnels, car tôt ou tard, toutes les technologies, aussi obsolètes et peu avancées soient-elles pour l'instant, fonctionneront assez bien pour être implantées. Par conséquent, la solution idéale serait de créer une technologie sans perdant, qui renforcerait à la fois la protection des renseignements personnels et la sécurité. Les responsables des politiques doivent indiquer aux fabricants d'appareils les types de technologies dont ils ont besoin, et trouver des solutions pour renforcer la sécurité tout en protégeant les libertés.

2 A complete transcript of the Minister's speech is available on the Citizenship and Immigration Biometrics Forum Web site: **http://cic-forum.ca/english**

À la suite de son exposé, le Pr Dershowitz a répondu à un certain nombre de questions posées par les participants au Forum. Plusieurs d'entre eux sont revenus sur le thème de la reptation de fonction (la pente glissante), et se sont dits préoccupés par le fait que cela constitue un danger inévitable advenant l'adoption d'une carte d'identité nationale. Il a répondu que le but de tenir un débat approfondi et transparent sur ces questions est de s'assurer que la reptation de fonction n'est pas permise ou, au pire, qu'elle se produise après la tenue de ce débat. Selon lui, il est toujours préférable de faire les choses au grand jour plutôt qu'en cachette. Ainsi, son dernier conseil aux participants a été le suivant : peu importe la façon dont agit le Canada à l'égard de la carte d'identité nationale, il doit faire preuve de transparence. Il ne faut pas attendre que quelque chose de bien résulte du statu quo, mais utiliser la technologie pour résoudre des problèmes et protéger le bien public. En outre, il est important de ne pas rejeter la technologie en se disant que de bonnes choses résulteront de l'inefficacité de la technologie.

Discours d'ouverture – L'honorable Denis Coderre Ministre de la Citoyenneté et de l'Immigration du Canada

Le ministre Coderre a commencé son discours en déclarant que le débat sur la carte d'identité nationale et sur l'utilisation de la biométrie était très important pour les Canadiens[2]. Il a indiqué que malgré les divergences de points de vue des participants au Forum, certaines questions ont une portée internationale et doivent faire l'objet d'un débat constructif qui permettra au pays d'aller de l'avant. Le « train de la biométrie » a quitté la gare, et cette question doit être examinée dans un esprit d'ouverture.

M. Coderre a relevé certaines questions clés auxquelles le Canada devra répondre dans un avenir rapproché, notamment la façon d'améliorer l'intégrité des documents, de contrer le terrorisme et l'usurpation d'identité et de s'adapter aux nouvelles exigences internationales. L'intégrité des documents est une question qui concerne tous les pays; les États-Unis, l'Organisation de l'aviation civile internationale et le G8 prennent d'ailleurs des mesures à cet égard. Nous devons donc nous demander si, en tant que Canadiens, nous voulons mettre au point nos propres solutions à ces problèmes, ou laisser les autres pays nous imposer leurs méthodes. La planète rapetisse sans cesse et les pièces d'identité prennent de l'importance en présence des réalités que sont la sécurité et le terrorisme.

Une question étroitement liée à ce débat, selon le Ministre, est de déterminer si le Canada peut à la fois protéger les renseignements personnels et renforcer cette protection, tout en augmentant la sécurité et en vérifiant l'identité. D'après lui, la réponse est claire : cela est effectivement possible. Toute la question de l'intégrité des documents compte de plus en plus, étant donné que les Canadiens s'attendent à ce que leur gouvernement soit en mesure de leur garantir que les personnes qui viennent au Canada sont celles qu'elles prétendent être. De plus, ils veulent que les documents qui leur donnent accès à des services soient résistants aux altérations et à la fraude et qu'ils conservent leur intégrité avec le temps.

Évidemment, l'adoption d'une carte ne permet pas de régler tous les problèmes; la carte fait partie d'un large éventail de mesures qui compte également une solution à l'usurpation d'identité, qui, selon le Conseil Canadien des Bureaux d'éthique commerciale, coûte 2,5 milliards de dollars par année aux Canadiens. Aux États-Unis, la Commission fédérale du commerce a évalué que 10 millions d'Américains avaient été victimes de tels crimes au cours de la dernière année. Des données statistiques indiquent que près de mille personnes par mois signalent un cas d'usurpation d'identité aux autorités policières, sans compter les cas non rapportés. Par conséquent, si le coût du projet de carte d'identité nationale peut

2 Le Document d'information et d'autres documents ayant trait au Forum sur la biométrie se trouvent dans le site Web créé par CIC pour l'occasion : **http://cic-forum.ca/francais**.

sembler élevé, l'absence de mesures de protection des citoyens et de l'économie signifie également des dépenses considérables.

Le ministre Coderre a indiqué que le gouvernement comprend la nécessité d'agir. Citoyenneté et Immigration Canada est en voie de délivrer deux millions de nouvelles cartes de résident permanent, carte qui a reçu un bon accueil. L'utilisation de la biométrie est de plus en plus répandue, et plusieurs provinces envisagent d'introduire des indicateurs biométriques dans les pièces d'identité, notamment la lecture rétinienne et les empreintes digitales dans le permis de conduire. Aux États-Unis, les pressions s'accentuent pour que le gouvernement adopte un permis de conduire standard, contenant des caractéristiques biométriques. Certaines mesures sont également prises relativement à la sécurité dans les aéroports. Il importe aussi d'agir dans le domaine de la protection des renseignements personnels, comme le veut l'entrée en vigueur de la nouvelle *Loi sur la protection des renseignements personnels* et les documents électroniques.

De plus, le gouvernement fédéral a adopté une approche mieux coordonnée relativement à ces questions et c'est à CIC qu'il revient d'en assumer la responsabilité. Ne rien faire et espérer que tout se passe pour le mieux n'est pas une possibilité. Le Ministre a brièvement décrit deux grandes approches éventuelles pour améliorer l'intégrité des documents :

- Une nouvelle approche globale à l'échelle nationale, où la possibilité d'une carte d'identité nationale serait envisagée;
- L'amélioration graduelle des pièces d'identité de base existantes.

Selon lui, quelle que soit l'approche adoptée, il faudra trouver le moyen de créer une carte (ou des cartes) qui mettra à profit les technologies à notre disposition et tiendra compte des pratiques exemplaires. L'approche globale pourrait s'inspirer de celle adoptée par plus d'une centaine de pays qui possèdent une carte d'identité nationale. Le Comité permanent de la citoyenneté et de l'immigration à la Chambre des communes se penche déjà sur ces approches et a examiné la question sous tous ses angles. Fondamentalement, il se demande si une approche globale est préférable à une approche progressive. Autrement dit, est-ce qu'une carte d'identité nationale pourrait remplacer la panoplie de cartes dont se servent actuellement les Canadiens?

Le ministre Coderre a poursuivi en affirmant que le Canada pourrait également choisir une approche graduelle qui consisterait à améliorer les pièces d'identité déjà en vigueur, et considérer la biométrie dans le cadre de ce processus. Il est important de noter que les Canadiens possèdent déjà de nombreuses cartes qui fournissent des renseignements au gouvernement; il ne faut donc pas confondre le désir d'anonymat (que les Canadiens ne possèdent pas actuellement) et le désir de protection des renseignements personnels. Des changements ont déjà commencé à être apportés aux pièces d'identité des Canadiens, comme dans le cas du permis de conduire qui est désormais en plastique et muni d'une photo, et ces changements deviendront monnaie courante. Les noms de Canadiens se retrouvent dans un grand nombre de bases de données et beaucoup d'individus et d'organisations possèdent un nombre considérable de renseignements personnels sur de nombreux Canadiens. Pour résoudre cette situation, le Canada a deux options principales : maintenir le statu quo relativement à la protection des renseignements personnels de la population ou étudier toutes les possibilités qui s'offrent à lui pour trouver un juste équilibre entre le renforcement de la sécurité et la protection des renseignements personnels.

Concernant l'identification des immigrants ayant obtenu le droit d'établissement au Canada, le ministre Coderre a indiqué que la nouvelle carte de résident permanent était plus pratique et sécuritaire que l'ancien formulaire. Néanmoins, il croit que la sécurité de cette dernière pourrait être renforcée grâce à l'ajout d'indicateurs biométriques, qu'elle a la capacité de contenir. Par contre, certaines questions importantes demeurent sans réponse :

Comment procéder pour rendre plus sécuritaires les pièces d'identité?

Comment protéger les renseignements personnels et prendre en compte les préoccupations concernant l'atteinte aux libertés fondamentales?

Quel serait le coût d'une carte d'identité nationale?

Une analyse coûts-avantages permettant de prévoir avec précision les dépenses publiques et l'économie que représenterait la carte a-t-elle été faite?

Concernant ce dernier point, le Ministre a indiqué qu'il est important, dans un premier temps, de s'entendre sur les concepts, puis de discuter du coût. La première question qu'il faut se poser est de savoir si les Canadiens veulent une carte d'identité nationale. Cette question pourrait être formulée ainsi : à quoi devraient ressembler les futures pièces d'identité et de quelle façon pourrait-on en certifier l'authenticité? Si les Canadiens sont d'avis que la carte d'identité nationale pourrait se révéler un outil utile, le gouvernement doit procéder à une analyse coûts-avantages et à une analyse de rentabilisation relativement à sa mise en œuvre. Selon les dires du Ministre, la carte de résident permanent sera délivrée à environ deux millions de personnes et le coût net de sa mise en œuvre est évalué à 22,9 millions de dollars.

Le ministre Coderre a affirmé que le Canada a besoin d'un débat public éclairé sur l'adoption d'une carte d'identité nationale et que le gouvernement doit présenter les faits et les questions au grand jour. Une décision reposant sur une politique d'intérêt public rationnelle, qui résultera en des améliorations concrètes aux yeux des Canadiens, doit être prise. Pour terminer, il a posé la question de pure forme suivante : pourquoi Citoyenneté et Immigration Canada est-il l'hôte d'une telle conférence? Il a répondu que, premièrement, son ministère a le devoir d'explorer les implications de toutes nouvelles technologies qui pourraient avoir une incidence sur son mandat et l'aider à mieux le remplir. Deuxièmement, le Canada doit regarder au-delà de ses frontières, soit vers les États-Unis, le Royaume-Uni, l'Union européenne, l'Australie et la Nouvelle-Zélande, afin de tirer des leçons de leur expérience et d'examiner les répercussions de leurs mesures sur le Canada.

Les Canadiens doivent aller au-delà des questions de technologie liées à l'adoption d'une carte d'identité nationale et réfléchir aux problèmes d'ordre public qu'elle permettrait de résoudre afin de déterminer si cela justifie son adoption. Nous pouvons nous doter des meilleurs outils, mais si nous adoptons une politique erronée, nous sommes condamnés à l'échec. L'utilisation de la biométrie comme moyen d'identification ou de vérification doit permettre de protéger les renseignements personnels et les libertés, ainsi que donner accès aux Canadiens aux données les concernant, afin d'en assurer l'exactitude et d'en empêcher l'utilisation frauduleuse.

Le Canada dispose d'une base solide sur laquelle construire en fonction de ses choix de politiques. Sa Charte des droits et libertés et son appareil judiciaire lui permettent de garantir qu'il ne deviendra pas un état policier. Nous avons la possibilité de créer un cadre législatif concernant l'utilisation de la biométrie dans les pièces d'identité. La biométrie est à nos portes; déjà, les Européens laissent tomber les simples cartes d'identité pour adopter des cartes à puce qui donnent accès aux services offerts par le gouvernement. Cette question touche tous les aspects de la vie quotidienne et nécessite des solutions globales.

En conclusion, le ministre Coderre a indiqué que la discussion qui se tiendra au cours du Forum sur la biométrie servira à élaborer des solutions en matière de politique pour le gouvernement et l'aidera à discuter de ces questions avec ses collègues ministériels et ses homologues internationaux. Il s'agit d'un des plus importants débats de la prochaine décennie. Le gouvernement a la responsabilité de tenir un débat large et sérieux afin de veiller à ce que le Canada s'adapte au 21^{e} siècle.

Conférencier d'honneur : Biométrie – Passé, présent et avenir – Colin Soutar, Ph. D.
Conseiller technique en chef
Association canadienne de technologie de pointe – Groupe sur la biométrie
Directeur de la technologie, Bioscrypt Inc.

M. Soutar a commencé son exposé en indiquant que l'utilisation de la biométrie dans le cadre d'une carte d'identité nationale prête à la controverse. Par conséquent, il a décidé de se concentrer sur certaines questions ayant trait à l'utilisation de la biométrie conjointement à la création et à la mise en œuvre d'une carte d'identité, et de discuter de certains efforts de normalisation relatifs à la biométrie entrepris au Canada et dans le reste du monde.

Dans cet esprit, M. Soutar a indiqué qu'il est nécessaire d'examiner certains facteurs primordiaux lorsque vient le temps de prendre une décision relative au type de technologie biométrique qui convient à une application donnée. En fait, il soutient qu'il est très important de comprendre deux ou trois points délicats concernant les répercussions de la biométrie sur un système dans son entier, qui ont une incidence profonde sur la mise en œuvre appropriée des technologies biométriques.

À titre d'exemple, M. Soutar a examiné certaines des initiatives actuellement en œuvre au niveau international relativement à la normalisation de la biométrie. Il a indiqué que l'Organisation internationale de normalisation s'intéresse vivement à l'utilisation de la biométrie et qu'un de ses comités travaille actuellement à l'établissement de normes internationales en matière de biométrie. Le Canada ferait d'ailleurs figure d'avant-coureur dans le domaine de l'évaluation des dispositifs de sécurité et les Canadiens (dont lui-même) participent à la définition de ce qui, dans le futur, sera la norme à l'échelle mondiale.

M. Soutar a relevé les empreintes digitales, l'iris, les mains et la géométrie du visage comme étant les quatre indicateurs biométriques revenant le plus souvent dans le cadre de l'établissement de normes internationales et de la mise en œuvre commerciale. Il a précisé qu'il était important, particulièrement du point de vue de la perception du public, que la biométrie ne serve pas à identifier une personne, mais plutôt à reconnaître que cette personne a été enregistrée dans le système auparavant, grâce à une recherche dans une base de données ou une mise en correspondance directe. La biométrie ne peut pas servir à permettre d'identifier une personne qui n'est pas déjà inscrite dans le système, mais peut permettre d'établir un lien entre un identificateur du système et cette personne.

Dans un système bien défini, la biométrie peut à la fois procurer une sécurité accrue et protéger la confidentialité. Il appartient au public de déterminer le degré d'équilibre acceptable entre la protection des libertés fondamentales et le renforcement de la sécurité qui sera introduit dans le système. Un exemple de deux technologies différentes qui n'ont pas la même incidence sur la protection des renseignements personnels est celui de la technologie de vérification et de la technologie d'identification des individus.

En termes simples, le processus d'identification a recours à une base de données pour établir l'identité d'une personne, alors que la vérification en différé ne fait que démontrer qu'une personne correspond à un « identificateur » inscrit sur une carte. M. Soutar affirme qu'il est possible d'enregistrer de l'information servant à la vérification localement (sur une carte), tandis que l'identification doit faire appel à un système centralisé qui possède une base de données. Selon lui, un des principaux défis des systèmes d'identification est de devoir trouver un moyen simple et efficace de retirer les droits et privilèges des titulaires de carte.

L'utilisation de la biométrie devrait être complétée par le chiffrement et les cartes à puce pour que sa mise en œuvre soit optimale. Autrement dit, pour pouvoir créer un système efficace, il faut combiner les technologies. Actuellement, une plus grande variété de technologies biométriques qu'auparavant sont mises en œuvre, et combinées de façon novatrice. En voici quelques exemples :

Confirmation de l'identité – utile partout où un passeport ou un NIP est demandé (par exemple, cartes d'appels interurbains, transactions bancaires, autorisation d'entrer dans un édifice).

Contrôle de l'accès – M. Soutar donne l'exemple d'American Express qui, à son siège social, a adopté une carte à puce renfermant des données biométriques afin de vérifier les allées et venues de ses employés (vérifier avec précision qui fait quoi dans l'immeuble, à quel moment). Cette carte est propre à l'entreprise et permet d'avoir accès aux différentes installations de l'entreprise. Le service de police de New York (NYPD) utilise également cette technologie.

Enregistrement de l'heure – une autre fonction des cartes contenant des indicateurs biométriques est l'enregistrement de l'heure et de la présence. Si un certain nombre d'employés ont accès à un coffre-fort muni d'un système biométrique, il est possible d'identifier avec précision les employés qui se trouvaient à cet endroit à un moment donné.

M. Soutar a conclu cette partie de son exposé en déclarant que la biométrie n'est pas « chose du futur », qu'elle est en fait déjà réalité.

M. Soutar s'est ensuite penché sur la question de la différence entre les systèmes biométriques de vérification et d'identification. Selon lui, l'identification permet d'accomplir des tâches comme la vérification des antécédents et nécessite l'accès à une base de données centrale, tandis que la vérification permet, grâce à un ensemble de données sous la main, de vérifier en tout temps qu'une personne est la véritable titulaire d'une carte. Par conséquent, l'algorithme mathématique servant à établir la correspondance n'a pas besoin d'être le même. Par contre, une seule acquisition d'indicateurs biométriques peut remplir ces deux fonctions.

Un exemple de l'utilisation de la vérification pour protéger les renseignements personnels est l'établissement, par un utilisateur, d'une identité unique au moyen de documents de référence comme un certificat de naissance. Un identificateur du système (p. ex., le numéro de passeport) est lié au profil de vérification de l'utilisateur[3] afin de créer un compte. Dans ce cas, l'identificateur ne sert qu'à confirmer que la personne en possession de la carte est celle qu'elle prétend être, et les données biométriques ne permettent pas d'obtenir d'autres renseignements. M. Soutar a insisté sur le fait que la biométrie comme telle n'identifie pas les individus, mais reconnaît que ces derniers sont inscrits de façon légitime dans le système.

M. Soutar a indiqué qu'un système fondé sur la vérification biométrique permettrait d'intégrer uniformément la biométrie dans un système existant qui ne comporte aucun élément biométrique. Dans ce cas, le processus interne du système de base de données n'a pas besoin de savoir qu'un indicateur biométrique est utilisé pour confirmer l'identité du titulaire de la carte; ce système est toujours lié à un identificateur à part comme un numéro de passeport. Ainsi, les droits et privilèges d'une personne sont contrôlés par l'application, et non par les indicateurs biométriques, qui peut également les lui retirer facilement.

Selon M. Soutar, le recours à un identificateur et à un profil de vérification permet aussi d'éviter le problème du profilage[4]; tout ce que doit savoir le système est si le numéro de passeport enregistré est valide; il n'a pas à savoir si la personne en possession du passeport est son titulaire. Une fois que l'identité du titulaire de la carte est vérifiée par le système qui confirme sa validité, le numéro de passeport correspondant est transmis à une application centrale, qui confirme à son tour la validité du passeport. La

3 Un profil de vérification est un ensemble unique de renseignements lié à un identificateur biométrique (p. ex., empreintes digitales) qui est inscrit sur instrument, comme une carte, qui pourra être comparé à un nouvel ensemble de données.

4 Se produit lorsqu'un agent désigne un individu ou un groupe d'individus comme devant faire l'objet d'une attention particulière en raison d'un identificateur comme la race.

mise en oeuvre d'un tel système signifierait que les agents n'auraient plus à prendre de décisions quant à l'admissibilité des personnes dans un pays; cette fonction serait remplie par un système central.

On peut donc se demander si un tel système peut être mis en œuvre tout en respectant la législation canadienne en matière de protection des renseignements personnels. Selon M. Soutar, le Canada possède des normes strictes en matière de protection des renseignements personnels. Les personnes qui seront inscrites dans un programme y auront préalablement consenti. Elles auront une idée de la raison pour laquelle un profil de leurs renseignements est créé. Deux principes relatifs à la protection des renseignements personnels sont particulièrement importants dans cette situation : le secret professionnel de l'utilisateur et la confidentialité des renseignements biométriques. Il importe donc de protéger le compte de l'utilisateur au moyen de la technologie de cryptage afin d'éviter l'altération du bloc de données. Les renseignements pourraient être enregistrés dans un code à barres, ce qui contribuerait grandement à l'intégrité du système.

M. Soutar a affirmé qu'un système de la sorte pourrait empêcher l'usurpation d'identité et entraver la capacité de certains individus de se servir de fausses identités pour perpétrer des actes terroristes. De plus, la séparation entre le profil de vérification de l'utilisateur et l'authentification du système diminue le danger de reptation de fonction.

M. Soutar a terminé son exposé en abordant les différents usages possibles de la biométrie dans l'avenir. Certains de ces usages nécessiteront la fusion de technologies biométriques pour des raisons de commodité et de sécurité, comme des systèmes à indicateurs faciaux et digitaux ou des systèmes à algorithmes multiples. Un autre progrès important, selon lui, sera la mise en œuvre d'algorithmes de liaison à clé, comme des profils propres à une application. Une autre amélioration serait la mise au point de jetons à puce pour applications multiples. Par exemple, un porte-clés pourrait contenir une multitude de clés donnant accès à un ordinateur personnel, à un compte bancaire ou à un autre appareil personnel et permettrait l'échange de renseignements personnels précis pour différents besoins.

Au cours de la discussion qui a suivi cet exposé, une question a été soulevée indiquant que le code utilisé dans les cartes (en l'occurrence le numéro de passeport) pourrait fournir des indices sur l'identité de son titulaire. M. Soutar a répondu, qu'en effet, l'identificateur ne possède aucune limite, et qu'il n'est même pas obligatoire qu'il prenne la forme d'un code. S'il convient mieux d'utiliser un nombre pseudo-aléatoire comme identificateur, cela peut se faire. En outre, il n'est pas nécessaire que le numéro soit visible sur la carte; il pourrait être chiffré pour plus de sécurité. Enfin, toujours selon M. Soutar, tous les systèmes peuvent faire l'objet d'abus et cette question devra être abordée dans le cadre du débat public sur ce sujet en général.

Un autre participant a demandé si les technologies d'identification pouvaient être utilisées en vue de réduire le nombre d'attentats terroristes. Plus précisément, il cherchait à savoir si la confirmation de l'identité pouvait empêcher un agent malicieux de commettre un acte regrettable, et ce, dans un environnement où des technologies biométriques d'identification sont en place. M. Soutar a répondu en affirmant que ces technologies peuvent renforcer la sécurité de plusieurs façons : en servant de moyen de dissuasion, en empêchant l'usurpation d'identité et, enfin, en demandant aux participants de subir un contrôle comme celui prévu pour l'obtention de la citoyenneté canadienne. Ce processus de vérification peut être lié à la capacité de retirer très rapidement certains privilèges, au besoin.

Première réunion d'experts – La biométrie dans le contexte international

Martin Giles, directeur adjoint, Service d'immigration du Royaume-Uni, Home Office

Gillian Russell, Direction générale, Justice et affaires intérieures, Commission européenne

W. Russell Neuman, Ph. D., analyste principal des politiques, Bureau de la politique scientifique et technologique de la Maison-Blanche

Gerry Van Kessel, coordonnateur, Consultations intergouvernementales sur les politiques d'asile, de reconnaissance du statut de réfugié et de migration en Europe, en Amérique du Nord et en Australie

Le but de cette réunion du matin était d'offrir un aperçu des différentes applications de la biométrie dans les autres pays. Les trois premiers experts ont été invités à parler de l'expérience de leurs territoires respectifs (le Royaume-Uni, l'Union européenne et les États-Unis), tandis que le quatrième expert est un Canadien qui œuvre à des questions d'immigration et de protection des réfugiés dans un contexte multilatéral.

Martin Giles
Directeur adjoint
Service d'immigration du Royaume-Uni, Home Office

M. Giles a commencé son exposé en déclarant que le terrorisme est un problème international, qui nécessite la coopération de tous les pays. Il a poursuivi en parlant de sa participation à l'élaboration et à l'exécution d'un programme d'identification biométrique relatif à l'immigration au Royaume-Uni. Pour M. Giles, l'établissement de l'identité dans le processus d'immigration est une question complexe qui, traditionnellement, reposait sur le passeport pour identifier une personne, connaître son nom, sa date de naissance et sa nationalité et obtenir certains renseignements sur ses déplacements antérieurs. Toutefois, ce système a commencé à s'effondrer lorsque, au cours des dernières années, de nombreux individus sont arrivés au Royaume-Uni sans pièces d'identité, qu'ils avaient détruites pour toutes sortes de raisons.

Selon M. Giles, le concept même d'identité est passionnant, du fait que la plupart des gens s'identifient par leur nom et l'endroit où ils vivent, alors que ces choses ne sont pas uniques et, par conséquent, ne peuvent servir de fondement à une identification précise. La biométrie offre la possibilité de démontrer l'unicité d'un être humain, mais ce, uniquement si celui-ci n'a pas déjà été enregistré dans le système. Le but du programme d'identification en immigration est donc de veiller à ce que chaque personne ne possède qu'une seule identité en vue de l'application du programme.

M. Giles a indiqué qu'en 1999, le Royaume-Uni prélevait manuellement les empreintes digitales des demandeurs d'asile. Ce système était très lent et ressemblait à celui utilisé par Scotland Yard (c.-à-d. la police). Il fallait six mois pour procéder à la vérification d'empreintes digitales, ce qui était considéré comme un délai inacceptable. La décision a donc été prise, à la fin des années 1990, de reconstruire le système. Au cours de leurs discussions, les responsables des politiques se sont demandé s'ils devaient continuer à utiliser les empreintes digitales comme identificateur ou adopter une nouvelle norme. Pour un certain nombre de raisons, la décision a été de continuer avec les dossiers dactyloscopiques, notamment parce que les empreintes digitales sont uniques, le SAID (Système automatisé d'identification

dactyloscopique) est une technologie essayée et éprouvée, il existe déjà des dossiers, un droit prévu par la loi permet l'échange de renseignements avec d'autres organismes (en particulier les services de police), le personnel est déjà formé pour prélever les empreintes digitales et ces dernières sont acceptées comme éléments de preuve.

L'objectif premier du programme consistant à automatiser le prélèvement des empreintes digitales aux fins d'asile, comme l'a brièvement indiqué M. Giles, était de pouvoir procéder à des examens dactyloscopiques n'importe où et d'obtenir les résultats de ces vérifications dans l'heure qui suit. Ces paramètres reposaient sur l'expérience opérationnelle des gestionnaires du projet. Conséquemment, aujourd'hui, chacune des unités de vérification des demandeurs d'asile possède cinq appareils de lecture par balayage et lecteurs de cartes qui peuvent balayer à l'encre les empreintes digitales. Ces appareils sont reliés à des unités de vérification rapide qui se servent de la technologie GSM (une technologie sans fil de seconde génération) et utilisent des téléphones cellulaires pour se brancher au système central. Le premier projet pilote est depuis devenu un programme à part entière, dans le cadre duquel des cartes biométriques reliées à l'EURODAC (base de données à l'échelle de l'Union européenne permettant de faire le suivi des demandes d'asile; il en sera question à la prochaine section de ce rapport) ont été produites. Le projet pilote a également résulté en un projet semblable comportant des liens directs avec le système de la police et prévoyant l'utilisation de ces données dans le cadre des demandes de visa. Enfin, M. Giles a indiqué que les cartes produites par ce système ont permis de corriger une faille dans le système d'immigration, qui permettait aux demandeurs d'asile de changer leur nom et de présenter des demandes multiples.

Du point de vue de M. Giles, le programme s'avère une réussite – le nombre de demandes multiples est passé de 6 % à 1 % du nombre total de demandes; les vérifications rapides permettent régulièrement d'identifier des meurtriers, des violeurs et d'autres criminels au moment où ils entrent dans le système; et les rapports sur les demandes permettent de faire diminuer les versements au titre des services nationaux d'aide à l'asile et de décourager les gens à demander à un mandataire de présenter une demande en vue d'obtenir ces services. Eurodac a également identifié plus de 1 100 demandes présentées par une tierce partie, et une récente étude a démontré que le système détecte près de 60 % des demandeurs multiples.

M. Giles a affirmé qu'un débat vigoureux prenait place sur le choix des données biométriques à utiliser de façon permanente dans le cadre de ce programme. Par ailleurs, selon lui, les avantages sont réels et tangibles. Il a indiqué certains domaines de politique pour lesquels on envisage d'avoir recours à la biométrie, notamment :

- prévention en matière de création d'identités multiples;
- réduction de la fraude en matière d'avantages;
- gestion des rapports;
- visa biométrique;
- vérification de sécurité accélérée;
- sécurité interne au sein des services d'immigration (contrôle d'accès et anticorruption);
- passeport biométrique.

M. Giles a conclu sa présentation en énonçant certaines des leçons tirées du programme :

- un taux d'exactitude de moins de 100 % pour ce qui est de la détection est acceptable étant donné que le système peut repérer près de 90 % des cas;
- la production de cartes d'identité est ardue lorsqu'elle est de divers ressorts, mais il est possible de surmonter ce problème;
- de réelles économies peuvent être réalisées en utilisant un système de carte biométrique de façon appropriée; mais la biométrie étant une nouvelle technologie, il y a encore une profonde ignorance à l'égard de son utilisation et de ses répercussions;
- des normes internationales sur la biométrie doivent être établies pour que nous soyons en mesure de travailler dans un contexte intergouvernemental. Aucun système de document, aussi bon soit-il, ne se compare à la reconnaissance de l'iris ou à la dactyloscopie;
- enfin, la bonne gestion et la bonne administration sont essentielles à la réussite du projet.

Gillian Russell
Direction générale, Justice et Affaires internes
Commission européenne

Le principal point de mire de la présentation de Mme Russell était le système Eurodac dont l'Union européenne se sert présentement pour assurer le suivi des demandes d'asile présentées sur son territoire. Mme Russell a particulièrement mis l'accent sur certaines des applications existantes de ce système, sur certaines des questions entourant sa mise en place réussie, et sur certaines des nouvelles applications pour lesquelles l'UE envisage utiliser une base de données biométriques.

Mme Russell a commencé sa présentation en soulignant l'importance des politiques publiques dans la création d'un système comme Eurodac. À cette fin, elle a indiqué qu'Eurodac a été créé en tant que personne morale seulement après 10 ans de débat sur la meilleure façon de trouver un moyen rapide pour déterminer si une personne a présenté une demande d'asile dans plus d'un État membre à la fois. Compte tenu du genre de données utilisées dans le système, la participation du Danemark a été exclue, mais la Norvège et l'Islande y participent et on s'affaire à négocier l'adhésion de la Suisse. Elle a souligné qu'Eurodac est la première base de données biométriques européenne permettant à différents pays d'utiliser leurs propres renseignements exclusifs. En fait, chaque pays peut utiliser son propre système pour stocker des renseignements sur les empreintes digitales, où elles ont été prélevées, et sur le sexe de la personne concernée; il n'est pas nécessaire de fournir le nom ni la photo de la personne concernée au moment de transférer des données biométriques dans Eurodac.

Mme Russell a déclaré qu'il y a trois catégories de données utilisées avec Eurodac :

> **Catégorie 1** - demandeurs d'asile de plus de 14 ans (les données sont conservées pendant 10 ans);
>
> **Catégorie 2** - personnes interceptées au moment de franchir une frontière externe de façon irrégulière (les données sont stockées au besoin);
>
> **Catégorie 3** - personnes illégalement présentes dans un État membre (aux fins de vérification du statut d'asile).

Dans la catégorie 3, il est possible de procéder à l'identification à l'aide de deux empreintes digitales, tandis qu'il est nécessaire d'avoir 10 empreintes pour les autres catégories. Les États membres recueillent les données et les transmettent à un endroit (point d'accès national) qui, à son tour, les envoie à l'unité internationale. Mme Russell a indiqué que les données du système Eurodac sont transférées via l'IPRPV, un

réseau semblable à Internet entièrement encodé. De plus, elle a indiqué qu'il n'y a que trois personnes qui travaillent avec ce système et que le délai de réponse à une requête n'est que de cinq minutes. Le système a été déployé en janvier dernier et devrait être instauré dans 10 autres pays l'année prochaine. Pour ce qui est de la disponibilité, le système ne peut être mis hors fonction que pendant quatre ou cinq minutes par période de 28 jours, ce qui est très exigeant en matière de niveau de service.

Mme Russell a donné un aperçu de certaines des différentes applications pour lesquelles l'UE envisage d'utiliser des technologies semblables, comme le système utilisé pour présenter une demande de visa d'entrée dans un État membre. Le problème commun devant être résolu au sujet de ce système est qu'il est très complexe de vérifier et d'identifier les personnes qui ont présenté une demande de visa d'entrée dans plus d'un État membre. Les systèmes de visa et Eurodac étant des systèmes très différents qui traitent des problèmes tout aussi différents, Mme Russel a indiqué qu'un certain nombre de défis techniques stimulants doivent être relevés avant qu'une application du genre puisse être utilisée. Elle a également mentionné que l'on espère que la biométrie permettra de trouver des réponses utiles à ces questions. À vrai dire, une proposition a été présentée concernant l'utilisation, dans un nouveau visa d'entrée, d'une puce supplémentaire dans laquelle seront stockées deux empreintes digitales qui ne serviront qu'à des fins d'identification.

Finalement, Mme Russell a fait part de quelques-unes de ses préoccupations à l'égard de la robustesse de certaines des nouvelles technologies proposées, en indiquant qu'elle n'est pas persuadée qu'il y a eu suffisamment de recherche pour évaluer leur efficacité. Elle a affirmé qu'il est nécessaire de s'harmoniser et que les systèmes ne seront pas en mesure d'interopérer si tous les États membres ne respectent pas une norme commune. Avec Eurodac, les données stockées appartiennent à l'État membre qui les a recueillies. Les États membres peuvent également stocker ces données eux-mêmes, s'ils le souhaitent. Elle a cependant précisé que, dans le futur, l'échange de données entre les États se fera en fonction d'une certaine forme d'uniformité, notamment un identificateur unique, et d'une norme commune; de nombreux forums, dont le G8 et d'autres organismes internationaux, se penchent sur cette question.

En conclusion, Mme Russell a déclaré que la mise en œuvre d'un tel système exige que les personnes concernées portent une attention particulière à la protection des renseignements personnels. Cet élément est présentement géré par des organismes indépendants en Europe. Elle a fait valoir que ces organismes peuvent examiner l'enregistrement chronologique des données pour ce qui est du versement et de l'extraction des données, ainsi que la période pendant laquelle on conserve les journaux ainsi créés. Elle a également indiqué qu'il est nécessaire, selon elle, de trouver un équilibre entre les droits des voyageurs et les divers objectifs techniques et opérationnels. À cette fin, l'UE effectue de nombreuses recherches pour tenter de s'assurer que les technologies développées et mises en œuvre aident à l'élaboration et à la mise en œuvre de bonnes politiques. L'UE déploie beaucoup d'efforts pour mettre en place une approche d'identification cohérente, incluant le développement d'un passeport pour les citoyens de l'UE.

Dr. W. Russell Neuman
Analyste principal des politiques
Bureau de la politique scientifique et technologique de la Maison-Blanche

La présentation de M. Neuman portait principalement sur la technologie et la sécurité des frontières. Il a amorcé sa présentation en indiquant qu'en raison de l'importance que revêt la biométrie, selon le département américain de la Sécurité intérieure, ce dernier s'efforce de concevoir des projets de recherche sur la biométrie dans le but d'accroître ses connaissances pour ce qui est de son utilisation et de ses applications dans un contexte de sécurité. Il a également mentionné que le département américain prend très au sérieux les préoccupations en matière de protection des renseignements personnels, comme le

prouve la présence d'un agent principal de protection des renseignements personnels, dont le mandat est législatif, pour conseiller le secrétaire responsable de ces projets.

M. Neuman a poursuivi en affirmant qu'à la Maison-Blanche, le Groupe de coordination de la biométrie du Conseil national de la science et de la technologie, en collaboration avec plus d'une douzaine d'autres départements d'État et organismes, se penche sur une série de questions concernant l'utilisation de la biométrie, notamment :

- modalités de la biométrie (empreintes digitales, iris, etc.);
- systèmes biométriques et interface humaine;
- regroupement des données biométriques, infrastructure d'essai et évaluation;
- questions sociales et juridiques, et protection des renseignements personnels.

M. Neuman a mentionné que le dernier groupe est très actif et qu'il porte fruit. Il y a cependant, selon lui, un certain nombre de questions de nature internationale qui n'ont pas encore été réglées.

En ce qui a trait à la suggestion qu'il y aurait un compromis à faire entre la protection des renseignements personnels et la sécurité, M. Neuman a déclaré que l'une n'excluait pas l'autre. Selon lui, la protection des renseignements personnels n'est pas synonyme d'anonymat, et ne peut pas être assurée si le système ne fonctionne pas de manière efficace. Il définit la protection des renseignements personnels comme la capacité d'examiner l'identité d'une personne et la façon dont on s'en sert. À ce titre, il a souligné que la protection de la vie privée est liée à la prévention de l'usurpation de l'identité et au contrôle de l'usage qui est fait des renseignements personnels. Pour M. Neuman, protéger les renseignements personnels signifie être en mesure de corriger une erreur ou de prévenir la fraude liée à une utilisation suspecte ou à une mauvaise utilisation des renseignements de la part des autorités. Dans ce contexte, il a donné un exemple de la façon dont la biométrie peut accroître la protection des renseignements personnels, comme lorsqu'une autorité vérifie un élément dans un système et que son pouvoir de le faire est également vérifié par l'entremise de l'utilisation de leurs propres identificateurs biométriques.

M. Neuman a parlé de la nécessité de trouver une solution « faite au Canada » et a cité, dans ce contexte, l'article 32 de l'Accord Manley-Ridge sur un programme conjoint de recherche. Selon lui, une des principales questions qui doit être réglée est l'utilisation de systèmes biométriques pour la protection des renseignements personnels et la sécurité commune. L'article 32 de l'accord susmentionné met l'accent sur ces deux aspects et se fonde sur ce qu'il perçoit comme une pression inopportune entre deux secteurs de politique publique.

M. Neuman a conclu sa présentation en suggérant certaines activités communes entre le Canada et les États-Unis. Il a donné en exemple le suivi d'une récente étude parrainée par la Maison-Blanche sur l'exactitude de l'identification non assistée par ordinateur, qui pourrait servir de point de départ pour des études subséquentes. Il a terminé en affirmant que la communauté de recherche ne dispose présentement d'aucun point de repère sur le nombre d'acceptations et de refus erronés dans les systèmes humains d'identification présentement utilisés.

Gerry Van Kessel
Coordinateur, Consultations intergouvernementales sur les politiques d'asile, de reconnaissance du statut de réfugié et de migration en Europe, en Amérique du Nord et en Australie

M. Van Kessel est un ancien fonctionnaire de Citoyenneté et Immigration Canada présentement en affectation à Genève. Il a amorcé sa présentation en précisant qu'il n'est pas un expert en biométrie. À ce titre, il a mis l'accent sur la gestion et la politique plutôt que sur les questions techniques entourant l'utilisation de la biométrie. Il a indiqué que la question entourant l'utilisation de la biométrie est trop importante pour être laissée entre les mains des experts, et qu'une difficulté propre à ce domaine tient au mystère et au caractère obscur qu'il recèle pour de nombreux gestionnaires.

M. Van Kessel a cité des exemples d'utilisation de la biométrie à l'échelle internationale. La biométrie est notamment utilisée pour faciliter le passage des frontières, en particulier dans les aéroports, par l'entremise de divers processus :

- identification des voyageurs de confiance;
- programme CANPASS à l'aéroport de Vancouver;
- programme INSPASS (Services d'immigration et de naturalisation) dans dix aéroports des États-Unis.

Il a souligné que des programmes semblables sont en place à Singapour, Tel-Aviv, Amsterdam, Zurich, Sydney et en Suède. L'Allemagne utilise la biométrie dans son processus de délivrance des visas et les États-Unis envisagent de faire de même, tout comme l'Union européenne. Le Haut Commissariat des Nations Unies pour les réfugiés (HCR) utilise ce système dans le programme de rapatriement des réfugiés afghans à partir du Pakistan, et l'Italie dispose d'une carte d'identité nationale renfermant des données biométriques. L'Organisation de l'aviation civile internationale se sert de cette carte comme pierre angulaire pour l'élaboration de certaines de ses normes internationales.

M. Van Kessel a déclaré que l'Organisation mondiale du commerce a discuté de cette question avec ses hauts dirigeants et experts, et a indiqué qu'il est absolument nécessaire de se garder au fait des nouveaux développements. Selon M. Van Kessel, puisqu'il est trop tard pour mettre la biométrie de côté, la question n'est pas de savoir s'il faut ou non avoir recours à la biométrie, mais plutôt de déterminer comment nous devons gérer son utilisation.

Comme l'a souligné M. Van Kessel, en immigration, la biométrie offre de nombreux avantages :

- elle offre l'avantage de mieux garantir l'identité;
- elle donne aux résidents et réfugiés autorisés une identité reconnue universellement;
- elle peut faciliter l'évacuation et le rapatriement des réfugiés;
- elle fait échec à la fraude et aux abus;
- elle préviendra la fraude dans les examens médicaux dans le cas des personnes devant se soumettre à un tel examen;
- elle rendra la non-coopération moins avantageuse;
- elle facilitera l'identification des criminels et des autres personnes constituant un risque;
- elle donne un identificateur unique permettant de rendre plus efficace le traitement des cas.

M. Van Kessel a indiqué qu'il n'y a pas que des avantages qui découlent de l'utilisation de la biométrie. Elle soulève également un certain nombre de défis, comme ceux qu'il a donnés en exemple :

- possibilité d'erreurs humaines lors de l'entrée des données;
- possibilité de commettre des méfaits;
- assurance de la qualité;
- nécessité d'offrir une formation régulière à l'intention des administrateurs des systèmes biométriques.

Selon M. Van Kessel, la biométrie ne règle pas le problème d'identité puisqu'il est possible de cacher son identité véritable au moment de l'enregistrement, et l'intégrité d'un système biométrique repose sur la qualité du processus d'enregistrement.

M. Van Kessel a affirmé que le problème entourant la protection des renseignements personnels exige que l'on convienne de garanties dès le début de la conception d'un système biométrique, afin de restreindre l'échange de données, la reptation de fonction et l'usage inapproprié des données. Il est d'avis que la biométrie ne doit pas restreindre la protection des renseignements personnels et que les fonctions prosécurité ne doivent pas affecter la protection des renseignements personnels. Pour M. Van Kessel, un des éléments importants est que le public n'est pas ouvert à toutes les technologies et, souvent, le public accepte une technologie donnée s'il peut en tirer un avantage. Il est donc important, selon lui, de savoir si la réalité sera aussi belle qu'on nous la laisse entrevoir, notamment en ce qui concerne l'amélioration de la sécurité. Les résultats sont-ils ceux que l'on escomptait? Par exemple, est-ce que la biométrie facilitera vraiment le passage à la frontière?

Il a poursuivi en disant qu'il y a deux catégories de gens qui tentent d'entrer dans un pays : ceux qui sont admissibles, et ceux qui sont interdits de territoire. Il n'y a pas deux mesures; une personne satisfait aux critères ou n'y satisfait pas. Un des éléments déterminants au moment de prendre cette décision est le fait que l'examinateur doit être convaincu de l'identité de la personne concernée. Les personnes qui répondent aux critères d'entrée n'ont aucune raison de tenter de se dérober à leur identification, tandis que celles à qui on refuse l'entrée peuvent tenter de se créer une nouvelle identité. Selon M. Van Kessel, ces personnes pourraient hésiter davantage à le faire si elles savent qu'on utilisera la biométrie pour confirmer leur identité.

M. Van Kessel a déclaré qu'il y a toujours eu de la fraude et de fausses déclarations en immigration, particulièrement dans des catégories comme la réunification des familles, les demandeurs d'asile et les étudiants qui ont l'intention de travailler. La fraude liée à l'identité et à l'immigration est très répandue aux États-Unis. Il a affirmé qu'il est étonnant de constater jusqu'où les gens sont prêts à aller pour cacher leur identité. Selon lui, nombreux sont les gens qui sont prêts au meilleur ou au pire pour entrer au Canada. Une question s'impose donc : que faire avec les personnes dont l'identité et les intentions sont inconnues?

La plupart des gens pensent que le fait de ne pas avoir de papiers d'identité augmente leurs chances de rester au Canada de façon permanente. M. Van Kessel a précisé que ce phénomène a pris de l'expansion au cours des 20 dernières années. L'augmentation du nombre de tentatives pour entrer au Canada par fraude est un indicateur convaincant qu'il devient pressant de commencer à trouver des moyens pour réduire l'incidence de l'immigration illégale. Selon lui, tous les pays doivent relever le défi de créer des documents à l'épreuve de toute contrefaçon.

M. Van Kessel a affirmé qu'avant le 11 septembre 2001, les infractions aux lois de l'immigration étaient souvent perçues comme bénignes. Cette perception a toutefois changé et beaucoup de gens sont maintenant d'avis que le recours par les terroristes à la fraude liée à l'identité est un risque bien réel. La vraie question devient donc : comment identifier les personnes qui doivent être interceptées tout en

permettant aux autres de voyager comme bon leur semble? Selon lui, de nombreux éléments doivent être regroupés pour obtenir une approche qui fonctionne. La biométrie, combinée à des technologies permettant d'accroître la protection des renseignements personnels, semble offrir la meilleure possibilité de relever ce défi puisqu'elle offre les meilleures garanties pour ce qui est de l'identification d'une personne, et permet de comparer les identités vérifiées avec celles contenues dans une base de données centrale.

M. Van Kessel a conclu en déclarant que la biométrie aidera les agents de Citoyenneté et Immigration Canada à prendre des décisions justes et éclairées, et permettra de traiter les cas rapidement et avec efficacité. Bien utilisée, la biométrie aide les gouvernements à mieux gérer les mouvements de personnes. Mais il reste beaucoup de travail à faire avant que cette technologie ne puisse être instaurée à grande échelle.

Questions

Certains participants ont fait part de leurs préoccupations en ce qui a trait à la possibilité qu'une mentalité du « nous contre eux » ne se crée dans le cadre de l'instauration d'une carte biométrique, et à la tendance d'utiliser la biométrie pour faciliter l'obtention de privilèges pour les privilégiés et à titre de mécanisme de contrôle pour les personnes moins privilégiées. Les conférenciers ont répondu en indiquant qu'il y a, en général, un certain appui parmi les moins privilégiés en ce qui concerne l'utilisation appropriée des cartes biométriques, comme l'utilisation de données biométriques dans les fiches d'inscription au Royaume-Uni. Pour certains, les cartes s'avèrent un moyen pour concrétiser les avantages rapidement et facilement – non seulement le processus est-il plus rapide quand on utilise des cartes contenant des données biométriques, mais les personnes honnêtes présentant des demandes authentiques veulent habituellement avoir en leur possession un document stable prouvant leur statut. D'un autre côté, les cartes peuvent servir à protéger les demandeurs honnêtes en excluant les personnes qui présentent des demandes non légitimes.

Un autre point soulevé par une conférencière était qu'il n'y a aucune statistique sur l'étendue du recours abusif au système par les réfugiés, bien que l'on puisse lire, dans tous les quotidiens de l'UE, des histoires entourant des cas d'abus. Selon elle, l'utilisation d'un système biométrique, comme Eurodac par exemple, pourrait permettre de réfuter certains de ces mythes en fournissant des données crédibles et exactes. Finalement, un troisième conférencier a indiqué qu'il y a un réel problème de politique en ce qui a trait à l'équilibre entre les droits des réfugiés et le droit d'un pays à limiter la migration. Le conférencier a affirmé que les gouvernements doivent régler les questions de politique avant de penser aux aspects techniques.

Un autre participant a demandé que l'on élabore au sujet du mécanisme de surveillance en matière de protection des renseignements personnels concernant les systèmes décrits par les conférenciers. Un conférencier a répondu qu'il existe un bureau européen de protection des données pour l'UE, ainsi que divers bureaux nationaux indépendants de protection des données. Ces bureaux effectuent des vérifications et les bureaux de protection des données peuvent assurer le suivi des transactions et préciser pendant combien de temps un bureau d'immigration doit conserver des données archivées. Un deuxième conférencier a ajouté qu'il y a, au Royaume-Uni, une obligation juridique de se conformer à la *Loi sur la protection de l'information*.

Une dernière question concernait la possibilité d'utiliser des systèmes d'identification comme moyen, pour le gouvernement, d'identifier les personnes qui font du harcèlement ou qui commettent des abus. Encore une fois, les conférenciers ont répondu en mettant l'accent sur la possibilité que les systèmes biométriques permettent d'introduire une forme d'objectivité dans le processus en faisant en sorte que la décision en matière d'identification ou de vérification de l'identité soit prise par l'intermédiaire d'un système impartial comme Eurodac, plutôt que par un garde ou un agent d'inspection.

Un des conférenciers a résumé la question entourant la possibilité d'utiliser abusivement les cartes d'identité nationales en demandant, pour la forme, s'il y avait des antécédents d'inégalités aggravantes de la technologie. Selon les conférenciers, il n'y en a pas puisque la biométrie facilite l'accès des personnes honnêtes aux services dont elles ont besoin, tout en rassurant le public en général que les abus sont minimisés. Pour ce qui est de savoir si la technologie peut servir de noirs desseins, le conférencier a répondu que toute technologie peut être utilisée de façon inappropriée, donc qu'il est important de tirer profit de la nouveauté et de l'intérêt à l'égard de la biométrie pour répondre aux questions fondamentales sur la gouvernance et le contrôle, et ce, afin de minimiser les possibilités d'abus.

Conférencier invité au déjeuner – Frank Graves
Président
Les Associés de recherche Ekos inc.

Le discours prononcé par Frank Graves, président des Associés de recherche Ekos inc. (EKOS), portait sur le résumé et les analyses d'une récente étude effectuée par EKOS sur la protection des renseignements personnels et sur la possibilité d'instaurer une carte d'identité nationale contenant des données biométriques. Les résultats divulgués lors de la présentation étaient fondés sur le témoignage de 16 groupes de consultation que EKOS a rencontrés au cours de la dernière année pour discuter de la protection des renseignements personnels. Les résultats correspondent à ceux obtenus à la suite d'un sondage général mené auprès de 3 000 Canadiens.

Le premier argument de M. Graves était que bien que les opposants à l'idée d'instaurer une carte d'identité nationale ont tendance à être plus convaincus que ceux qui sont en faveur, ils ne constituent pas une majorité de Canadiens. La recherche entreprise par EKOS indique que, si la situation est expliquée clairement, le public serait ouvert à l'inévitabilité et à la possibilité d'instaurer une carte d'identité nationale.

M. Graves a poursuivi en affirmant que bien que les Canadiens soient préoccupés par l'idée d'instaurer une carte contenant des données biométriques, particulièrement en ce qui a trait à la protection des renseignements personnels et à la compétence des gouvernements, ces préoccupations sont éclipsées par les problèmes évidents qu'ils constatent à l'égard du système actuel, et par d'autres éléments connexes. Selon M. Graves, il est clair que les Canadiens n'auraient pas répondu la même chose il y a dix ans. Les sondages menés par EKOS au début des années 1990 indiquaient que les Canadiens n'avaient pas les mêmes préoccupations (quantité et qualité).

Bien que les Canadiens soient d'avis que la protection des renseignements personnels est importante et en péril, ils sont d'avis qu'ils sont en mesure de gérer ces menaces. À vrai dire, d'année en année, la protection des renseignements personnels préoccupe moins les Canadiens et cela est attribuable à l'augmentation de la confiance accordée aux nouvelles technologies. Les citoyens sont également moins préoccupés parce que les prédictions d'intrusion technologique et d'échec catastrophique ne se sont pas réalisées. M. Graves a noté que malgré le fait que les préoccupations entourant la protection des renseignements personnels aient diminué considérablement au cours des dernières années, elles sont plus importantes depuis le 11 septembre 2001. Il a cependant indiqué que, bien que la situation concernant la protection des renseignements personnels se soit replacée dans la plupart des cas depuis cet événement, les Canadiens sont toujours très préoccupés par la sécurité. Par ailleurs, la confiance du public à l'égard de l'autorité pouvant s'occuper des questions liées à la protection des renseignements personnels s'est déplacée du secteur privé au secteur public. En fait, la confiance à l'égard du secteur public augmente à ce sujet.

M. Graves a allégué que l'opposition orwellienne à l'égard du risque d'intrusion dans la vie privée par le gouvernement est une réalité dont l'impact est de moins en moins important sur les Canadiens des

générations montantes. Environ 75 % des répondants des générations montantes étaient d'accord avec l'affirmation suivante : « Ça ne me dérange pas que les gouvernements utilisent des renseignements qui me concernent, tant et aussi longtemps que je sais pourquoi et que je peux demander que cela cesse. Lorsque l'on remplace le mot « gouvernements » par le mot « entreprises », le ton change. En effet, en 1992, 71 % des répondants étaient d'accord avec cette affirmation, tandis que seulement 40 % des répondants le sont aujourd'hui.

M. Graves a également déclaré que les Canadiens semblent croire que la dichotomie apparente entre la protection des renseignements personnels et la sécurité est fausse. Ils ne perçoivent pas ces questions comme incompatibles et exigeront que l'on accorde une grande importance à chacune d'entre elles. Ils ne sont toutefois pas convaincus que de mauvaises choses se produiront et ils veulent savoir quelles garanties et mesures sont en place.

M. Graves a par la suite indiqué que, depuis le 11 septembre 2001, de nombreux effets sur la population s'étant manifestés auparavant, comme l'opposition au fait d'accueillir des immigrants originaires de certains pays, se sont maintenant dissipés. Il semble par contre y avoir une réaction défavorable permanente pour ce qui est des immigrants originaires des pays arabes, et les gens semblent être favorables au profilage racial. L'opinion est revenue aux niveaux d'avant le 11 septembre dans plusieurs secteurs, notamment l'économie et les sentiments à l'égard de l'État, mais les répercussions sur les questions liées à la protection des renseignements personnels et à la sécurité semblent vouloir se perpétuer.

En ce qui concerne l'évaluation du risque, comme l'instauration d'une taxe dans les aéroports et l'installation de caméras de surveillance, les Canadiens semblent être prêts à faire certains compromis précis. M. Graves a d'ailleurs allégué que les Canadiens semblent se ranger derrière la sécurité et qu'ils ne semblent pas trop se préoccuper du terrorisme au Canada. Il a indiqué que les répondants sont également préoccupés par la relation entre le Canada et les États-Unis – 50 % des Canadiens sont d'avis qu'il y a un nombre considérable d'activités terroristes au Canada. Puisque l'appui à l'égard d'une carte d'identité nationale ne semble pas être affecté, dans un sens, par le fait que le Canada pourrait vivre des moments difficiles, il semble important, selon M. Graves, de comprendre d'où vient l'appui à l'égard d'une telle carte au sein de la population canadienne.

Les sondages menés par EKOS au cours de la dernière année ont révélé qu'environ 50 % des Canadiens sont d'avis que le gouvernement protège relativement bien les renseignements personnels et n'abusera pas des pouvoirs qui lui sont octroyés, comparativement à 25 % des répondants qui ne sont pas d'accord avec cette affirmation. M. Graves a indiqué que ceux qui sont contre ont cependant tendance à s'exprimer vertement. Tant au Canada qu'aux États-Unis, une pluralité de la population croit que l'on doit accorder davantage de pouvoirs aux policiers. Si cette idée est présentée avec l'affirmation que le Canada doit octroyer plus de pouvoirs pour lutter contre le terrorisme, une nette majorité de répondants appuient la délégation, à cette fin, d'autres pouvoirs aux policiers ou aux organismes de renseignements.

M. Graves a indiqué que la nature des préoccupations à l'endroit d'une carte d'identité nationale semble principalement être philosophique – les Canadiens ne doivent pas compromettre la protection des renseignements personnels des générations à venir pour protéger leur sécurité. Les Canadiens semblent être très préoccupés par le sacrifice des libertés fondamentales de la prochaine génération. En gardant cet aspect en tête, il semble que la sécurité ne soit pas le principal facteur influençant l'appui à l'égard d'une carte d'identité nationale; on s'inquiéterait autant de la possibilité d'abuser du système actuel. Les Canadiens comparent les avantages découlant d'une carte contenant des données biométriques et le genre d'abus perpétrés à l'endroit du système actuel.

M. Graves a indiqué que non seulement la majorité des Canadiens appuient l'instauration d'une carte d'identité nationale, mais que plus les répondants en apprennent au sujet de la biométrie grâce aux sondages menés par EKOS, et plus ils entendent parler des pour et des contre d'une telle carte, plus ils

ont tendance à renforcer leur appui à l'égard de la carte. Seulement 6 % des Canadiens sont d'avis que le recours abusif aux pièces d'identité n'est pas une question importante.

Une question a été posée relativement à la possibilité que l'adhésion à la carte soit volontaire ou obligatoire. M. Graves a affirmé que tout ce qui est offert sur une base volontaire a tendance à recevoir un appui plus important que ce qui est obligatoire, mais l'écart est minime. Les participants au sein des groupes de consultation appuyaient davantage la carte obligatoire parce qu'ils étaient d'avis que les criminels et les personnes qui abusent du système ne se procureront pas une carte sur une base volontaire.

M. Graves a affirmé que lorsque l'idée de l'utilisation de la biométrie a été lancée en association avec celle d'une carte d'identité nationale, l'opinion est devenue nettement plus favorable à une carte d'identité. Les aspects positifs d'une carte d'identité nationale sont les suivants pour les Canadiens : elle peut réduire les abus et les fraudes, constitue un moyen d'identification plus précis que ceux qui existent actuellement, peut contribuer à la sécurité et pourrait aider à maintenir l'accès au marché américain. Les questions touchant la protection de la vie privée, le coût et les risques possibles de dérapage figuraient parmi les aspects négatifs.

M. Graves a conclu que le gouvernement devait avoir des arguments solides pour faire accepter l'instauration d'une carte d'identité nationale. Les Canadiens veulent comprendre comment et pourquoi elle sera instaurée, quelles seront les conséquences pour les citoyens et comment elle sera utilisée. Le public croit également que l'adoption d'une telle carte est inévitable, de sorte que le gouvernement ferait tout aussi bien de s'organiser en conséquence dès maintenant. Le public appuie l'utilisation de la biométrie pour réduire les fraudes et les abus auxquels se prête le système. En même temps, il reste une grande inquiétude face aux utilisations par le secteur privé, comme la sélection des candidats à un emploi (les transactions commerciales inquiètent davantage que l'utilisation des données par le secteur public).

Enfin, M. Graves a fait valoir que près de quatre-vingts pour cent des Canadiens pensent que l'utilisation de technologies biométriques est inévitable. Dans cette optique, le public est très favorable à la création de meilleurs documents d'identité, et voit la carte d'identité nationale comme un moyen parmi beaucoup d'autres possibles. Actuellement, les arguments pragmatiques en faveur d'une carte semblent éclipser les arguments philosophiques contre. Peu de Canadiens prônent activement l'adoption d'une carte d'identité nationale biométrique, mais ils reconnaissent en général qu'une telle carte pourrait être nécessaire et estiment que la fonction publique est apte à régler les questions de protection de la vie privée, si l'adoption d'une telle carte devenait une nécessité impérative.

Certains des participants ont exprimé des réserves au sujet de l'étude et de la méthode utilisée, estimant que les questions étaient biaisées en mettant l'accent sur la sécurité, l'utilisation de la biométrie et les répercussions du terrorisme. Selon eux, la technologie n'est peut-être pas la seule solution. M. Graves était d'avis, comme eux, qu'il fallait se garder d'une surutilisation de la technologie pour régler les problèmes. Il a indiqué que lorsqu'on a demandé aux Canadiens comment le Canada devrait régler la question du terrorisme à long terme, ils ont effectivement indiqué comme étant les deux principaux moyens un meilleur service du renseignement et le développement d'une société plus multiculturelle et plus tolérante.

Conférencière de l'après-midi : Questions liées à la protection des renseignements personnels – Stéphanie Perrin
Présidente
Société Discrétion digitale

Mme Perrin a commencé son exposé en déclarant qu'elle allait essayer de cerner la question de la protection des renseignements personnels dans le contexte d'une carte d'identité nationale plutôt que du point de vue de la technologie. Un des principaux points qu'elle a fait valoir était qu'après le 11 septembre 2001, il y a eu une forte demande de technologies, et que cette technologie existait déjà avant les événements du 11 septembre, mais qu'il n'y avait pas de marché. À la suite du 11 septembre, des questions comme l'accès à des renseignements personnels par des organismes d'exécution de la loi et d'autres questions liées à l'application régulière de la loi, ont été reléguées au second plan au point que des technologies qui sont extrêmement invasives ont pu être utilisées plus facilement et dans certain nombre de contextes.

Mme Perrin estime que la liberté d'expression est absolument fondamentale et que la démocratie ne peut survivre sans elle. Bien qu'elle soit d'accord avec M. Dershowitz qui, la veille, a déclaré que s'en remettre à une technologie fragile était pure folie, elle a précisé qu'il y avait actuellement un débat important dans la société civile sur la ligne de conduite qu'il convient d'adopter face à ces questions. Elle rappelle que ce ne sont pas seulement les activistes défenseurs des droits humains qui critiquent la conception d'une carte biométrique, mais également les experts de la sécurité et de la technologie eux-mêmes.

Un des principaux points qu'a fait valoir Mme Perrin était que se précipiter vers une solution sans définir le problème était toute une gageure. Elle se demande donc pourquoi le Canada se précipite sur la solution de la biométrie. La biométrie est une mesure logique dans le cas du contrôle des frontières, mais dans beaucoup d'autres cas, elle n'a pas forcément de raison d'être. Il faut se poser certaines questions, par exemple : S'agit-il d'authentifier l'identité d'individus? De vérification de leur identité? Demandons-nous une preuve d'identité alors qu'une carte « anonyme » mais sûre pourrait faire le même office? À son avis, il y a de nombreuses façons de régler le problème de l'usurpation d'identité, par exemple, mettre fin au crédit facile, et d'autres mesures que prônent les défenseurs de la vie privée. Rien n'oblige à mettre en œuvre une mesure aussi invasive qu'une carte d'identité nationale.

Selon Mme Perrin, les Canadiens doivent placer la question de la carte d'identité nationale dans le contexte du marché actuel, étant donné l'appétit de données sur les transactions. Mme Perrin a demandé s'il fallait laisser les lois du marché dicter la demande de données. Elle a cité l'échec des mécanismes de surveillance comme un problème majeur lié à l'instauration de systèmes biométriques. Les lois sur la protection des renseignements personnels à elles seules ne permettent pas de protéger la vie privée étant donné que la collecte de données elle-même pose un problème et que les organismes de surveillance n'ont pas suffisamment de ressources, voire pas de ressources du tout, pour s'acquitter de leur rôle de protecteurs du citoyen dans le contexte des technologies avancées de protection. Elle a également exprimé certaines préoccupations : des ressources suffisantes seront-elles consacrées à l'instauration d'une carte d'identité nationale? Il existe, en théorie, des façons de régler les problèmes de protection de la vie privée, mais elles coûtent de l'argent, et l'argent ne sera probablement pas au rendez-vous lorsque les systèmes seront mis en place. Par ailleurs, elle craint que les cartes ne soient utilisées à d'autres fins.

Mme Perrin a laissé entendre qu'il était malhonnête de discuter de la question d'une carte d'identité nationale en la présentant comme autre chose qu'un système, faisant partie d'un continuum. Le Canada s'engage sur la voie de la carte d'identité nationale sans avoir d'abord fait la recherche nécessaire. Elle fait également remarquer que le droit à la vie privée faisait partie d'un ensemble de droits connexes dans la Charte des droits et libertés et dans la Déclaration universelle des droits de l'homme, et que d'autres

droits fondamentaux, comme la liberté de circulation et la liberté d'association, étaient également menacés par une carte d'identité nationale.

Après cette discussion sur la relation entre une carte d'identité nationale et différents droits, M^me^ Perrin a examiné le concept d'une telle carte par rapport à dix principes de la protection de la vie privée. Selon elle, l'obligation de rendre compte est très importante, la détermination des fins de la collecte des données également, mais il n'était pas réaliste de croire que le principe du consentement de la personne concernée pouvait être respecté dans le cas d'une carte d'identité nationale. Elle a déclaré que les cartes facultatives avaient tendance à devenir très vite obligatoires, ce qui était peu compatible avec le principe du consentement. Elle pense également que l'exactitude est une arme à double tranchant, dans la mesure où elle peut être utilisée pour porter atteinte à la vie privée, qui est la raison pour laquelle les défenseurs de la vie privée préfèrent quelquefois que des données peu exactes soient recueillies, parce que moins de personnes pourraient s'y fier pour les utiliser à d'autres fins.

Le principe de l'accès est fondamental également, dans la mesure où une personne doit pouvoir voir et contester les données entrées dans les systèmes biométriques si l'on veut garantir l'intégrité de ces données. Elle a fait remarquer qu'au Canada il n'était même pas nécessaire d'être visé par des données pour pouvoir en contester la collecte et la codification dans des bases de données en vertu de la *Loi sur la protection des renseignements personnels* et les documents électroniques. Cette loi apporte en particulier une solution au fait que, souvent, seuls les experts de la sécurité ou des systèmes peuvent voir ce qu'il advient des renseignements personnels.

M^me^ Perrin a déclaré qu'une caractéristique fondamentale de la biométrie alarmait beaucoup de gens, soit le fait qu'elle se rapporte au corps. Par ailleurs, les données biométriques ne peuvent pas être révoquées si elles ont été compromises. La révocation est un problème et un défi clés pour tout système d'authentification, spécialement les systèmes biométriques. Si le flux binaire est compromis, le système biométrique doit permettre le réenregistrement du vrai sujet des données. Une des grandes difficultés liées à l'usurpation d'identité actuellement est la restauration de l'identité. Si un système biométrique est compromis, il est bien plus difficile de le changer pour rétablir l'identité d'une personne.

M^me^ Perrin craint qu'on ne demande aux citoyens une carte d'identité nationale pour prouver leur identité dans le cadre d'un nombre croissant de transactions commerciales. Elle a cité le problème du numéro d'assurance sociale : on demande actuellement aux gens de produire leur carte de NAS à l'épicerie ou dans les magasins vidéo Blockbuster. Tous les établissements commerciaux veulent des cartes d'identité sûres, et l'instauration d'une carte d'identité nationale ne ferait qu'exacerber le problème. Elle a déclaré que dans une démocratie il y avait souvent des citoyens qui comprenaient très mal leurs droits et qu'il revenait donc au gouvernement de faire particulièrement attention à ce que ces droits soient respectés.

M^me^ Perrin a également mentionné les coûts massifs associés à l'instauration d'une carte d'identité nationale. Selon elle, les coûts ne suivront pas une croissance arithmétique proportionnelle au nombre d'individus visés, mais plutôt une croissance exponentielle. En outre, elle a affirmé que tout le concept de la surveillance était très important et que les exemples de cartes européennes qui ont été cités ne tenaient pas compte du fait que l'Europe avait une infrastructure de surveillance, par exemple, la Cour européenne des droits de l'homme, loi européenne sur la protection des données et commissaires indépendants. Nous n'avons pas ce genre de surveillance au Canada, ce qui amène à douter de la capacité du gouvernement d'assurer une surveillance indépendante de la conception et de l'instauration d'une carte d'identité nationale.

Les questions concernant la souveraineté, l'accès aux données et leur contrôle sont également des questions importantes pour Mme Perrin. Pour qu'un système soit sûr, il faut qu'il soit possible d'y accéder et qu'il y ait des contrôles humains. Pour illustrer son propos, elle a posé une question théorique : Qu'adviendrait-il si des données sur des Canadiens étaient stockées en Inde? Est-il possible de garantir

que les agents indiens répondent aux normes canadiennes en matière d'intégrité? Quels droits d'accès aux données les gouvernements étrangers auraient-ils? La réponse est simple : tous les gouvernements ont un droit d'accéder à des systèmes de données et d'en extraire des données, droit qui l'emporte sur celui de l'individu à la protection de sa vie privée. Étant donné qu'une carte d'identité nationale pourrait donner accès à une très grande quantité de données, le choix de la technologie ainsi que du mode d'entreposage et de gestion devient important. De l'avis de M^me^ Perrin, les politiques et les lois voulues pour protéger les données sont nécessaires, mais pas suffisantes. La collecte de données doit être soumise à des restrictions.

M^me^ Perrin a terminé son exposé par quelques suggestions sur la façon de faire avancer le débat sur la biométrie. Selon elle, il faut :

- amorcer un dialogue soutenu avec la société civile;
- cerner les problèmes, les définir et élaborer un cadre d'analyse;
- arrêter de promettre un monde sécuritaire au public; il est faux de dire que renoncer à la protection de la vie privée peut nous protéger du terrorisme; nous vivons dans un monde dangereux, et les gouvernements doivent le faire comprendre aux citoyens;
- effectuer une surveillance efficace;
- agir avec plus de transparence;
- faire les recherches préalables nécessaires.

Pendant la discussion qui a suivi l'exposé de M^me^ Perrin, un participant a déclaré que beaucoup de Canadiens allaient avoir des cartes biométriques prochainement, et qu'il était évident que le reste du monde s'en allait vers la même solution. À cet égard, le Canada a plusieurs options claires : ne rien faire, ou trouver une solution « typiquement canadienne ». Les Canadiens s'inquiètent des risques de dérapage et veulent des barrières de sécurité, mais beaucoup de gens utilisent déjà les technologies biométriques, et leurs craintes diminuent à mesure qu'ils en savent plus sur le sujet.

M^me^ Perrin a répondu que la marge de manœuvre pour concevoir une solution « typiquement canadienne » était limitée. Elle a déclaré que l'on pouvait faire valoir que certains groupes, comme les camionneurs, pouvaient avoir un seuil d'acceptation plus élevé à l'égard de l'utilisation de données biométriques que d'autres groupes, mais que cela ne devait pas signifier que la même norme soit appliquée dans chaque situation. Elle a conclu en disant que l'utilisation et la collecte de données devaient être adaptées aux fins auxquelles les données sont recueillies.

Un autre participant a conclu cette partie de la séance en déclarant qu'il y avait en réalité quatre critères de la protection de la vie privée :

- l'existence d'un mécanisme spécialisé de protection des données;
- une surveillance indépendante;
- une évaluation des facteurs relatifs à la vie privée;
- l'adoption d'autant de technologies de protection de la vie privée que possible.

Deuxième réunion d'experts : Biométrie – Comprendre et évaluer les incidences de la biométrie

Roger Gibbins, président-directeur général, Canada West Foundation

Jennifer Stoddart, présidente, Commission d'accès à l'information du Québec

Raj Nanavati, International Biometrics Group

Raymonde Folco, députée de Laval-Ouest

Le groupe de l'après-midi s'est concentré sur le thème : Comprendre et évaluer les incidences de la biométrie, dans le contexte d'une carte d'identité nationale.

Roger Gibbins
Président-directeur général, Canada West Foundation

M. Gibbins a commencé son exposé en disant que dans le contexte de l'après-11 septembre et compte tenu des préoccupations que suscite l'usurpation d'identité, l'utilisation de la biométrie semblait souhaitable et utile. Il a donc axé ses propos sur deux grandes questions :

(1) la nécessité d'une nouvelle carte d'identité nationale plutôt que l'intégration de données biométriques à des documents existants;

(2) les problèmes liés à l'instauration d'une telle carte.

Il a également précisé qu'il allait se limiter à l'exemple de la carte d'identité nationale et ne pas parler de la biométrie en général. Il a commencé par déclarer que l'intégration de données biométriques à une carte d'identité nationale semblait moins soulever la controverse que l'instauration de la carte en soi. La question qu'il faut se poser semble pour lui être la suivante : Pourquoi avons-nous besoin d'un troisième mode d'établissement de l'identité? À première vue, la nécessité n'en est ni apparente ni absolue. Un passeport modernisé pourrait être utilisé pour voyager, de sorte que l'instauration d'une carte d'identité nationale semble impliquer la nécessité d'une preuve d'identité au Canada même. Qu'est-ce que le gouvernement du Canada a en tête? Quand les Canadiens devront-ils montrer cette carte et à qui?

M. Gibbins s'est demandé si ce document d'identité national serait comme un passeport, un document que l'on laisse chez soi, ou comme un permis de conduire que l'on porte sur soi en tout temps. Il a cité l'exemple du numéro d'assurance sociale pour illustrer les risques de détournement d'un document de sa fonction première. Le public avait reçu des assurances : le numéro ne serait utilisé qu'à des fins limitées. Or, il a rapidement été récupéré par le secteur privé. M. Gibbins pense donc qu'une carte d'identité nationale, quelle qu'elle soit, passera rapidement des applications du secteur public à des applications dans le secteur privé.

À son avis, une nouvelle carte d'identité nationale deviendrait bientôt un instrument incontournable tant dans le secteur public que dans le secteur privé, la nouvelle « norme d'excellence » pour les transactions publiques et privées. Il est allé jusqu'à dire qu'elle deviendra même nécessaire pour effectuer certaines transactions. Il s'agit, selon M. Gibbins, de veiller à ce que les renseignements intégrés à la carte ne soient pas utilisés à mauvais escient et à ce que le public ne pense pas qu'ils seront utilisés contre lui à un

moment ou à un autre. Il a cité les mises en garde d'Orwell contre les dangers d'une utilisation de l'information à mauvais escient.

Il a utilisé l'exemple de la sévérité de la nouvelle politique voulant qu'on ne sourie pas sur la photo de passeport. Elle n'a pas d'importance sur le plan technique, mais elle en a sur le plan politique. L'utilisation de données biométriques est peut-être inévitable, mais l'instauration d'une carte d'identité nationale ne l'est pas.

La question du caractère obligatoire ou non de la carte pose également un problème. Selon M. Gibbins, la carte pourrait devenir un signe de privilège ou un moyen de stigmatisation si elle n'était pas délivrée à tout le monde. Elle pourrait être un laissez-passer pour les gens qui voyagent en classe affaires ou un moyen de singulariser les nouveaux immigrants. En résumé, la carte ne serait pas utile à moins qu'elle soit obligatoire pour tous.

Une autre question soulevée par M. Gibbins est celle de savoir qui paiera la carte. Si ce sont les utilisateurs, le coût ne ferait que renforcer les divisions sociales. Pour lui, le coût général de l'instauration d'une carte posera également un problème et il ne faut pas croire aux estimations qui ont été faites. Il craignait également que les résidents des régions éloignées soient exclus. Enfin, il a soulevé la question du genre de renseignements qui seront apparents sur la nouvelle carte et pourquoi. Ces renseignements finiront-ils par être utilisés par le secteur privé? De son point de vue, même si les renseignements sont protégés d'une récupération à d'autres fins par le secteur privé, le public n'en verra pas moins dans la carte un lien vers d'autres utilisations. Il ne croira pas aux assurances données au sujet des barrières de sécurité ou n'aura pas confiance en l'efficacité de ces barrières.

M. Gibbins pense que l'instauration d'une carte d'identité nationale sera perçue comme l'enregistrement des armes à feu. Il a précisé, toutefois, qu'il était difficile de prévoir la réaction des Canadiens à l'utilisation d'une carte biométrique dans le système d'immigration. Certains pourraient être favorables à l'instauration de documents supplémentaires pour faire la distinction entre nous et les autres. Sur de nombreux plans, la valeur de la carte dépendra de son degré d'interopérabilité avec le système mis en place par le département américain de la Sécurité intérieure. Il est d'avis que si elle est pleinement intégrée au système américain, les Canadiens craindront que des renseignements ne soient ainsi révélés aux États-Unis, eux qui sont déjà réticents face à la transmission de renseignements aux autorités américaines. Selon lui, il faut d'abord régler toutes ces questions pour que l'instauration de la carte soit réussie.

De l'avis de M. Gibbins, l'adoption d'une nouvelle carte d'identité nationale se justifie en partie par la peur qu'ont les Canadiens de nouvelles menaces pour leur sécurité que pourrait leur réserver l'avenir. Il a, cependant, demandé si le besoin d'une sécurité accrue continuerait d'éclipser d'autres préoccupations à l'avenir.

Il a affirmé que l'une des façons de vendre aux Canadiens l'idée d'une carte d'identité nationale était de la leur présenter comme la solution au problème de la multitude de cartes qu'ils doivent porter sur eux actuellement. S'ils pouvaient utiliser cette carte pour faire tout ce que les autres cartes leur permettent de faire, ils pourraient être plus favorables à son instauration. Toutefois, une telle « supercarte », renforcerait les craintes profondes qu'ont déjà les Canadiens concernant la communication de renseignements personnels aux entreprises commerciales.

M. Gibbins a conclu son exposé en disant qu'il pourrait y avoir quelques réels avantages à une instauration progressive de la technologie biométrique.

Jennifer Stoddart
Présidente
Commission d'accès à l'information du Québec

D'entrée de jeu, M^me^ Stoddart a indiqué que le recours à la biométrie dans le contexte de la vérification d'identité fait l'objet d'une loi spécifique au Québec : la Loi concernant le cadre juridique des technologies de l'information. En réalité, a-t-elle souligné, la protection de la vie privée au Québec fait historiquement l'objet d'une attention particulière, par exemple, en 1982, l'Assemblée nationale a adopté la première loi sur la protection des renseignements personnels du Québec. C'est dans le cadre de cette initiative du gouvernement québécois que la question de la biométrie a été abordée pour la première fois. En effet, à la suite des événements du 11 septembre 2001, l'engouement pour la biométrie a confirmé le choix du Québec d'encadrer juridiquement son utilisation.

M^me^ Stoddart a déclaré que la Commission d'accès à l'information du Québec a toujours exprimé des réserves au sujet de l'instauration d'une carte d'identité nationale. Les premières discussions ont eu lieu au Québec par suite des inquiétudes provoquées par de possibles fraudes électorales dans certaines circonscriptions lors des élections provinciales de 1990; on avait alors examiné la faisabilité d'instaurer une carte d'identité québécoise. La Commission s'y était opposée, de même qu'à d'autres propositions subséquentes de carte d'identité universelle, et avait plutôt appuyé un certain nombre d'autres méthodes de vérification de l'identité, qui ont depuis été mises en œuvre avec succès.

La Loi concernant le cadre juridique des technologies de l'information du Québec renferme des dispositions particulières qui autorisent la Commission à surveiller et à contrôler les banques de caractéristiques et de mesures biométriques. L'objectif de la loi est d'établir un cadre régissant l'utilisation de ces informations, afin d'offrir notamment une certaine protection aux transactions électroniques, de normaliser les documents juridiques et de créer une équivalence fonctionnelle entre les documents électroniques et les documents papier. Dans certains de ces contextes, la question de l'authentification soulève un défi et M^me^ Stoddart reconnaît que l'utilisation de ces informations sur Internet comporte des difficultés sous le régime du droit civil du Québec. Cependant, des articles précis de la loi québécoise traitent spécifiquement du recours à la biométrie comme outil d'identification personnelle.

La biométrie est autorisée pour faire le lien entre les individus et les documents aux trois conditions suivantes :

1. L'identification biométrique ne doit pas porter atteinte à l'intégrité physique de l'individu.
2. Elle ne doit pas servir à localiser un individu, sauf pour des raisons de santé et de sécurité.
3. La personne concernée doit donner son consentement exprès et les données biométriques ne doivent servir qu'aux fins de vérification et de confirmation d'identité.

Bien que ces dispositions n'aient pas subi l'épreuve des tribunaux, elles s'inscrivent dans le contexte plus large des protections juridiques de la vie privée au Québec, notamment que le système juridique au Québec ne peut forcer une personne à donner un échantillon de fluide corporel et qu'il est interdit d'utiliser un dispositif pour localiser une personne.

M^me^ Stoddart a affirmé qu'au Québec il faut démontrer la nécessité d'utiliser des caractéristiques biométriques – le minimum requis – pour en faire l'application et que la saisie ne peut se faire à l'insu de la personne concernée. Le fait que la police puisse relever des empreintes digitales sans consentement ne peut être invoqué pour utiliser d'autres identificateurs biométriques. Les informations biométriques recueillies ne peuvent servir à quelque autre type de décisions ou fins, à l'exception de la vérification et de la confirmation de l'identité (par exemple, un test de dépistage de drogue ne pourrait être effectué en utilisant des informations biométriques recueillies pour une fin autorisée).

Pour M^me^ Stoddart, un autre élément important de la loi québécoise est le fait que l'information doit être divulguée à la personne concernée et que les identificateurs biométriques doivent être détruits dès que l'objectif visé a été atteint. L'un des aspects les plus novateurs de la loi, à son avis, est l'obligation de divulguer au préalable, à la Commission d'accès à l'information du Québec, l'existence de toutes les banques d'identificateurs biométriques – qu'elles soient ou non utilisées.

En décrivant les pouvoirs de la Commission en ce qui a trait aux banques d'identificateurs biométriques, M^me^ Stoddart a indiqué qu'ils sont en réalité plutôt limités – la Commission peut rendre une ordonnance concernant la conception des banques et peut en suspendre l'utilisation. Cependant, la Commission préfère se fier à une trousse d'auto-analyse à l'intention des administrateurs de bases de données et à un outil d'évaluation de l'impact sur la vie privée. Jusqu'à maintenant, a-t-elle dit, seulement quatre bases de données biométriques ont été développées et mises en service au Québec, notamment une base de données volontaires au centre athlétique de l'Université de Montréal, une base de données dans un milieu de travail syndiqué, qui a soulevé la question de la capacité du syndicat à donner son consentement au nom de ses membres, et une petite base de données biométriques dans un projet pilote d'Hydro-Québec, qui est utilisée pour vérifier l'identité d'individus faisant de grandes transactions financières.

En conclusion, M^me^ Stoddart a déclaré qu'au Québec, le recours à la biométrie s'inscrit dans le contexte du respect de la vie privée, qui est reconnu comme un droit fondamental et comme une préoccupation prioritaire du législateur. Elle a soutenu que pour les gouvernements qui veulent instaurer des bases de données et des outils biométriques, des règles strictes doivent être arrêtées : notamment, le système doit être extrêmement sécuritaire et son développement et son utilisation doivent se conformer aux lois sur les droits de la personne et aux autres principes régissant la vie privée. Finalement, elle a mentionné que le système québécois devrait servir de modèle à tout le Canada, précisant que toute initiative doit comporter une fonction de surveillance assurée par des experts indépendants comme la Commission d'accès à l'information du Québec.

Raj Nanavati
Partenaire
International Biometric Group

D'entrée de jeu, M. Nanavati a indiqué que sa firme a élaboré un cadre BioPrivacy en 1999, en réponse aux demandes des clients et à d'autres indicateurs faisant ressortir le besoin d'élaborer un cadre de protection des renseignements personnels pour résoudre précisément les problèmes liés à la biométrie. Ainsi, ce modèle veille à ce que l'on tienne compte des préoccupations relatives à la protection des renseignements personnels dès le début dans le développement d'applications biométriques. La firme de M. Nanavati a été consultée au sujet du développement de la carte d'assurance-maladie de l'Ontario, que 12 millions de personnes possèdent, et la Maison-Blanche l'a également consultée au sujet du volet américain de l'initiative sur la frontière intelligente de l'Office of Science and Technology Policy, qui visera plus de 300 millions d'utilisateurs. Si un grand nombre d'individus utilisent un tel système, il est absolument essentiel d'adhérer à des exigences précises en matière de protection des renseignements personnels et à d'autres exigences en matière de politique.

Selon M. Nanavati, il faut d'abord déterminer en quoi la biométrie est reliée précisément aux préoccupations en matière de protection des renseignements personnels. En général, on parle de la protection de la vie privée et de la protection des renseignements personnels. Par conséquent, les décideurs doivent-ils considérer les données biométriques comme des renseignements personnels? À son avis, comme une empreinte digitale ne fournit aucun renseignement sur la personne à qui elle appartient, une interprétation très restreinte pourrait consister à conclure que les données biométriques ne sont pas des renseignements personnels. Il a cependant indiqué qu'il est souvent utile de voir ces questions sous

un angle plus général et d'aborder les questions relatives à la protection des renseignements personnels dans un contexte plus large.

M. Nanavati a ensuite discuté de l'importance des modèles et a notamment souligné l'importance de connaître la différence entre un modèle et une image. Il est extrêmement important de savoir de quel type d'image il s'agit. Une image peut être associée à une personne sur une base individuelle, alors qu'un modèle implique un changement unidirectionnel dans le but de créer une signature unique qui est différente de l'image d'une personne. Par conséquent, selon M. Nanavati, l'utilisation de modèles contribue à atténuer certaines des préoccupations au sujet de l'utilisation à mauvais escient des données.

M. Nanavati est également d'avis que l'utilisation de petits systèmes constitue un moyen important de protéger la vie privée. Les images sont interopérables, alors que la plupart des modèles ne le sont pas. Comme ils ne sont pas interchangeables, l'utilisation d'une technologie donnée lie un client à la technologie de ce fournisseur, ce qui réduit la capacité des parties extérieures à lire ou à interpréter cette information. Les répercussions sur la protection de la vie privée sont extrêmement importantes.

L'un des problèmes mentionnés par M. Nanavati était que les données biométriques peuvent changer avec le temps. C'est pourquoi la façon de mesurer la précision des technologies biométriques constitue une question importante. D'importants travaux ont été menés afin d'évaluer ces technologies de façon scientifique et rigoureuse, étant donné qu'elles sont utilisées par des centaines de millions d'individus. Un système biométrique peut commettre trois types d'erreurs de base : établir une fausse correspondance, établir une fausse non-correspondance et rejeter une inscription. Si un grand nombre de personnes ne peuvent pas s'inscrire dans un système, il faut alors avoir une autre forme d'identification; le système ne sert alors plus aux fins pour lesquelles il a été créé.

M. Nanavati estime qu'une surveillance très rigoureuse du processus d'inscription contribuera à réduire le taux d'échec à l'inscription. Toutefois, si l'on opte pour la mise sur pied d'un kiosque libre-service pour inscrire la population dans un système – une méthode comportant un taux d'inscription élevé – cela pourrait entraîner un taux d'échec de 10 p. 100. Le taux de précision dépend donc de la technologie utilisée et de ses applications particulières. Il y aura toujours des personnes qui ne pourront pas utiliser un identificateur donné (par exemple, un faible pourcentage de personnes n'ont pas un iris constant et ne peuvent donc pas s'inscrire à l'aide d'une technologie de reconnaissance de l'iris). Comme la biométrie n'est pas parfaite, il y aura toujours un certain taux de fausse correspondance. M. Nanavati a indiqué qu'il faut donc déterminer si la biométrie contribue à réduire le taux d'échec du système actuel. Par exemple, dans le cas des demandes d'immigration, il est important de veiller à ce que le taux d'échec des technologies biométriques soit plus faible que celui des méthodes traditionnelles d'identification visuelle.

M. Nanavati a poursuivi son exposé en précisant qu'on utilise quatre identificateurs pour évaluer une technologie – qu'il s'agisse de systèmes invasifs, neutres, restreints ou protecteurs. Les programmes gouvernementaux devraient à tout le moins utiliser des systèmes restreints. Dans ce contexte, M. Nanavati a présenté les trois principales fonctions BioPrivacy, telles qu'identifiées par sa firme :

- l'analyse des applications biométriques – cadre d'impact;
- l'analyse des technologies biométriques de base – risques de la technologie;
- les étapes vers un système restreint, respectant la vie privée – meilleures pratiques.

Il a expliqué que l'utilisation de ces critères pour évaluer une application biométrique assure un cadre d'évaluation objectif. Il a utilisé l'exemple de la technologie de reconnaissance faciale au Superbowl pour démontrer ce qui peut se passer lorsque ces technologies ne sont pas appliquées de façon uniforme. Au Superbowl, il y a eu de nombreux problèmes liés à l'utilisation de technologies biométriques, tels que l'absence de consentement de la part des participants – ce problème aurait pu être évité en indiquant sur

des affiches que des caméras intelligentes étaient utilisées. Selon M. Nanavati, il est important d'expliquer aux gens ce qui se passe vraiment et à quelles fins les renseignements recueillis seront utilisés.

Il y a énormément de confusion au sujet de la signification réelle du terme « biométrie ». C'est ce qu'ont démontré certains des groupes de discussion que l'organisation de M. Nanavati a dirigés. En général, les gens ont associé la dactyloscopie à la police. Cependant, une fois qu'ils en ont fait l'expérience, le taux d'inscription a été beaucoup plus élevé, ce qui a indiqué qu'ils étaient plus susceptibles d'accepter un identificateur biométrique après en voir fait l'expérience eux-mêmes. La vérification et l'inscription peuvent être très simples s'ils sont effectués de façon adéquate. Il semble que les gens ont besoin de faire l'expérience concrète des applications biométriques pour vraiment évaluer la faisabilité de cette technologie.

M. Nanavati a indiqué que le cadre BioPrivacy tient compte d'un certain nombre de facteurs, notamment :

- l'inscription facultative versus obligatoire;
- l'utilisation manifeste versus secrète de la technologie;
- l'utilisation à des fins de vérification versus d'identification;
- la durée fixe versus la durée indéfinie;
- le secteur privé versus le secteur public;
- l'individu versus l'employé;
- la propriété utilisateurs versus la propriété institutionnelle des données;
- le stockage personnel versus la base de données modèle;
- les identificateurs biométriques comportementaux versus physiologiques;
- le modèle versus les données identifiables.

Il a précisé que sa firme évalue le risque associé aux diverses applications en combinant ces facteurs.

En conclusion, M. Nanavati a indiqué que l'utilisation de la biométrie n'aurait en soi rien changé aux événements du 11 septembre 2001. Par contre, l'utilisation d'un système d'identification comportant des éléments biométriques aurait pu permettre aux organismes d'exécution de la loi de comparer les données avec les listes de signalement des criminels et des terroristes. Cependant, il n'existe actuellement aucune banque importante contenant la signature ou l'empreinte de l'iris de terroristes. C'est pourquoi il est important d'envisager sérieusement de recourir à ce genre de technologies dans le contexte de la lutte contre le terrorisme.

Raymonde Folco
Députée de Laval-Ouest

D'entrée de jeu, Mme Folco a établi la distinction entre une approche fondée sur les principes et une approche fondée sur les règles en matière de biométrie. Une approche fondée sur les règles énumère tous les maux sociaux qu'il faut résoudre, tels que la fraude liée à l'identité, le terrorisme et les abus du système, alors qu'une approche fondée sur les principes met l'accent sur les valeurs. Adopter une approche fondée sur les règles expose le gouvernement à de nombreux risques. Selon Mme Folco, plutôt que de mettre l'accent sur des affirmations comme la suivante : « si nous n'enfreignons pas la loi, nous demeurons à l'intérieur des limites de nos droits et obligations », le gouvernement devrait regarder les droits de toutes les parties concernées. Nous devrions nous demander « quelle ligne d'action fait

progresser le bien commun et appuie nos objectifs de confiance, de transparence et de saine gestion publique ».

Elle a ensuite identifié certains des instruments qui constituent le fondement de l'État canadien, notamment la Charte canadienne des droits et libertés et les garanties enchâssées dans la constitution canadienne. Les nouvelles mesures de sécurité qui ont été adoptées ont d'ailleurs limité certains de ces droits. En revanche, les nouvelles lois comme la *Loi sur la protection des renseignements personnels* et les documents électroniques (loi fédérale) et la *Loi sur la protection des renseignements personnels* (loi provinciale) protègent également le droit du citoyen au respect de sa vie privée. Cela dit, trois thèmes doivent être abordés : la sécurité, la protection de la vie privée et les droits de la personne ainsi que la relation qui existe entre ceux-ci. À son avis, la question importante à se poser est la suivante : quels sont les droits des parties concernées et quelle approche respecte ces droits? Plus le risque de violation de ces droits est élevé, plus les mesures à prendre doivent être sévères.

M^me^ Folco a déclaré que, dans le cadre du débat entourant la biométrie, l'attention a plutôt été tournée vers la sécurité, récemment, et que le forum sur la biométrie aurait eu lieu même si les événements du 11 septembre 2001 n'étaient pas survenus. En cette période d'après-guerre froide, alors que le climat est à la détente ouverte et à la collaboration, les Canadiens devront faire face à des menaces de terrorisme et d'usurpation d'identité prenant leur source ailleurs que dans l'État. Les progrès réalisés sur le plan économique et social sont liés à la mobilité accrue des individus, qui est à son tour liée à la capacité de ces derniers à prouver leur identité. M^me^ Folco a donc posé la question suivante : « quels sont les nouveaux risques et les risques continus, et où se situe la biométrie dans ce nouveau contexte axé sur la sécurité? »

En ce qui a trait au respect de la vie privée, M^me^ Folco s'est demandé si l'on en faisait assez pour informer les Canadiens des choix s'offrant à eux. La technologie est-elle un instrument ou plutôt un moyen d'arriver à une fin? Le respect de la vie privée est-il une valeur à préserver ou un état à atteindre? Jusqu'à présent, la biométrie a été décrite comme une atteinte absolue à la vie privée ou encore comme une mesure favorisant le respect de la vie privée. Toutefois, le gouvernement présente-t-il aux Canadiens le tableau complet de chacune des options, a-t-elle demandé? Quelle ligne d'action traite tous les individus de la même manière, appuie les principes de l'équité et de la justice, et permet aux citoyens de prendre leurs propres décisions et d'influer sur le cours de leur vie? Pouvons-nous nous fier aux résultats des sondages pour déterminer les mesures à prendre? Qu'en est-il de la majorité silencieuse – les points de vue exprimés reflètent-t-ils ceux de la population en général? Dans quelle mesure les sondages sont-ils nécessaires pour avoir une idée de l'opinion publique? Les défenseurs des citoyens semblent dire « non » à une carte d'identité nationale, mais dans quelle mesure sont-ils représentatifs de la population en général? Qui représentent-ils? En bout de ligne, quels compromis le public est-il prêt à faire pour obtenir autre chose en retour? Il s'agit d'une question importante dans l'application d'une carte d'identité nationale. M^me^ Folco est d'avis que tous les faits doivent être présentés aux citoyens pour leur permettre de prendre une décision éclairée.

La question des droits de la personne est tout aussi importante et soulève trois questions clés : y a-t-il des répercussions différentielles sur différents groupes (par exemple, sur les groupes religieux)? Quelle sorte de société cela encourage-t-il? Quels sont les outils disponibles pour limiter ces répercussions?

En conclusion, M^me^ Folco a demandé quelle ligne d'action reflète le bien commun. Elle est d'avis que la question à poser est la suivante : les Canadiens ont-ils l'honnêteté, le courage, la compassion, le sens de la justice, le contrôle d'eux-mêmes et la prudence pour affronter la menace réelle du terrorisme au Canada et pour éviter les généralisations racistes? Le Canada a-t-il besoin d'une nouvelle lentille biométrique pour aider les autorités dans des situations où un indicateur purement objectif est utile? À quoi servent la Loi sur la protection des renseignements personnels et la *Loi sur la protection des renseignements personnels*

et les documents électroniques, et à quoi sert la Charte si les gens ne se sentent pas en sécurité lorsque des mesures sont prises pour protéger leur vie privée?

La question demeure donc la suivante : le Canada doit-il adopter une approche fondée sur les principes ou une approche fondée sur les règles pour la carte d'identité nationale? Selon M^me^ Folco, le recours à la biométrie constituera une amélioration uniquement si les principes et l'éthique deviennent une partie intégrante de l'approche adoptée et sont respectés à chacune des étapes du processus. Le Canada doit déterminer le prix qu'il attache à l'être humain et à sa dignité, évaluer le produit offert et comparer les avantages par rapport aux coûts et par rapport aux risques. La législation doit protéger les Canadiens. Mme Folco a terminé son exposé sur la phrase suivante : « Contrôlons la technologie plutôt que de la laisser nous contrôler ».

Questions

Les participants ont amorcé leur discussion avec les experts en leur posant des questions au sujet des affirmations selon lesquelles les applications des technologies biométriques ne sont pas encore « au point ». L'un des experts a répondu que tout cela dépend du besoin de précision – qui dépend à son tour de l'application. Par exemple, la ville de New York utilise depuis plusieurs années la dactyloscopie pour identifier les bénéficiaires d'aide sociale. L'utilisation de la reconnaissance faciale dans les aéroports ne s'est pas avérée efficace, puisque cette technologie n'a pas permis d'identifier les terroristes. Les photos étaient prises à une distance de 20 pieds et comportaient des ombres et un mouvement, ce qui les rendait moins claires. Il y a des situations où cette technologie ne fonctionne pas. Il faut donc évaluer chaque situation et déterminer si cette technologie est une solution valable.

Un autre participant a mentionné la nécessité de mener des vérifications indépendantes permanentes de certaines des lois intrusives qui ont récemment été adoptées par le gouvernement. Le groupe d'experts a répondu que, actuellement, le Secrétariat du Conseil du Trésor du Canada soumet au Commissaire à la protection de la vie privée tous les projets du gouvernement ayant des répercussions sur la vie privée, et que cette surveillance devrait être plus rigoureuse dans le secteur privé. Un autre expert a indiqué que le Parlement agit en fonction de ce que les Canadiens veulent. Par conséquent, il faudra éventuellement examiner attentivement la législation sur la protection des renseignements personnels et ses répercussions sur la vérification et l'authentification.

Un dernier participant a indiqué que, dans le cadre de cette séance, on avait beaucoup discuté de l'utilisation de la biométrie aux fins du jumelage des réfugiés et des demandeurs d'asile. Il a déclaré qu'en tant que citoyen canadien, il ne se présente pas à la frontière pour être admis au pays, mais on continue néanmoins de lui dire qu'il doit avoir une carte d'identité pouvant servir à des fins de contrôle à l'intérieur des frontières canadiennes. Il estimait que l'on n'avait pas justifié la mise en œuvre d'une telle carte. L'une des experts a indiqué qu'il s'agissait d'un point très important. Elle a indiqué que le forum sur la biométrie était une initiative du ministre de la Citoyenneté et de l'Immigration, qui est le responsable fédéral sur les questions d'intégrité des documents. Elle a terminé en disant que quelqu'un devait soulever la question, puisqu'elle n'avait pas encore été abordée. Toutefois, dans l'avenir, un groupe plus large composé de représentants d'autres ordres de gouvernement et de citoyens, de partout au pays, devra déterminer le type de politique qu'il souhaite en matière d'identité.

Conclusions et orientations concernant les éventuelles mesures à prendre – L'honorable Denis Coderre Ministre de la Citoyenneté et de l'Immigration

La séance s'est terminée par une allocution prononcée par l'honorable Denis Coderre. Le ministre Coderre a d'abord repris les propos de son discours d'ouverture, affirmant qu'il s'agit d'une question très importante tant à l'échelle nationale qu'internationale. Il a mentionné que plusieurs membres du Comité permanent de la citoyenneté et de l'immigration de la Chambre des communes avaient assisté au Forum et que cela avait permis de briser la glace et d'entamer un débat national sur la question.

Pour M. Coderre, l'utilisation de la biométrie constitue une question fondamentale affectant tous les Canadiens. Citoyenneté et Immigration Canada a pris l'initiative d'ouvrir un débat national parce qu'il est responsable de la délivrance des documents d'identification primaires au sein du gouvernement fédéral, notamment les documents de citoyenneté et les documents liés à la résidence permanente (la nouvelle carte feuille d'érable). Le Ministre a déclaré que l'on utilise actuellement la biométrie et que l'on continuera de le faire. La question n'est pas de savoir « si », mais plutôt « quand ». Comme cette éventualité est inévitable, le ministre Coderre estime que le Canada doit commencer à penser à cette question et à en débattre, et que la population canadienne doit discuter de la question d'une carte d'identité nationale. Il estime que les identificateurs biométriques ne devraient pas viser uniquement les immigrants admis et les résidents permanents, mais également tous les Canadiens.

Selon lui, l'usurpation d'identité, la sécurité des frontières et les normes internationales sont autant de raisons d'envisager le recours à la biométrie. Il s'agit d'une question d'intérêt canadien nécessitant une approche équilibrée, mais le statu quo est hors de question. Il a dit estimer qu'un certain nombre de conditions nécessaires étaient en place : un régime de protection de la vie privée solide et de bonnes relations de travail institutionnelles dans le domaine de la protection de la vie privée. Il aime le modèle du Québec, consistant à fournir des mesures de protection législatives pour les utilisations autorisées de la biométrie, puisqu'il tient compte des réalités actuelles. En tant que ministre responsable, il est tenu de couvrir tous les angles et d'évaluer toutes les possibilités. Le débat national est ouvert et doit se poursuivre.

Le ministre Coderre a indiqué que le Canada doit veiller à ce que ses documents soient sûrs tout en assurant la protection des renseignements personnels et le respect des valeurs des Canadiens. Au cours des cinq prochaines années, le Canada aura besoin d'un million de travailleurs qualifiés, et d'ici 2026, la croissance démographique du pays sera entièrement attribuable à l'immigration. Le Canada doit garantir l'intégrité de ses documents primaires et protéger l'identité de ses citoyens, afin de relever les défis que pose cette nouvelle vague d'immigration. D'autre part, le Ministre a reconnu qu'il s'agit d'une question complexe et que le gouvernement devra élaborer des modèles ainsi que des stratégies concernant les coupe-feu, afin de protéger les renseignements personnels et d'améliorer la sécurité.

Mentionnant le caractère évolutif de cette question, le ministre Coderre a cité l'exemple de l'utilisation de pièces d'identité avec photo qui, il y a plusieurs années, a suscité beaucoup de controverse. Il a demandé aux participants de s'imaginer tentant de monter à bord d'un avion sans pièce d'identité avec photo, de nos jours. Il a indiqué qu'en tant que pays, nous devons absolument examiner la question de la collecte de renseignements et de l'utilité des bases de données. Le forum sur la biométrie n'était qu'un début, puisqu'il y aura d'autres étapes, mais ce fut un bon départ. Il a dit attendre avec impatience le dépôt du rapport final du Comité permanent de la citoyenneté et de l'immigration. Finalement, les Canadiens s'adapteront et trouveront une solution « typiquement canadienne » au sein du village planétaire.

ANNEXE II : ORDRE DU JOUR

Le mardi 7 octobre 2003 (Hôtel Fairmont Château Laurier)

HEURE	ACTIVITÉ
17 h 15	**Inscription**
17 h 30	**RÉCEPTION**
18 h	**DÎNER**
19 h 20	**Discours d'ouverture :** *Trouver un juste équilibre entre la sécurité et les libertés publiques* *Alan M. Dershowitz* *Professeur de droit* *Harvard Law School*

Le mercredi 8 octobre 2003 (Centre national des arts)

7 h 45	**Inscription**
8 h 20	**Annonces du matin**
8 h 40	**Observations préliminaires** L'honorable Denis Coderre Ministre de la Citoyenneté et de l'Immigration
9 h	**Orateur principal** Colin Soutar, Ph.D. Conseiller technique principal Association canadienne de technologie de pointe – Groupe de la biométrie Conseiller technique principal Bioscrypt Inc.
9 h 45	**Sondage instantané – Première séance**
10 h	**PAUSE**
10 h 20	**Première réunion d'experts : La biométrie dans le contexte international** Martin Giles, Directeur adjoint Service d'immigration du Royaume-Uni Gillian Russell, Direction générale Justice et affaires intérieures Commission européenne W. Russell Neuman, Ph.D., Conseiller principal en matière de politiques, Bureau de la politique scientifique et technologique de la Maison-Blanche Gerry Van Kessel, Coordonnateur des Consultations intergouvernementales sur les politiques d'asile, de reconnaissance du statut de réfugié et de migration en Europe, en Amérique du Nord et en Australie

12 h	**DÉJEUNER**
12 h 50	**Conférencier invité au déjeuner** Frank Graves Président Les Associés de recherche EKOS Inc.
13 h 30	**Points relatifs à la protection de la vie privée** Stephanie Perrin Présidente Société Discrétion digitale Inc.
14 h	**Deuxième réunion d'experts : Biométrie – Comprendre et évaluer les incidences** Roger Gibbins, Ph.D. Président et PDG Canada West Foundation Jennifer Stoddart Présidente Commission d'accès à l'information du Québec Raj Nanavati Associé International Biometric Group Raymonde Folco Députée de Laval-Ouest
15 H 30	**PAUSE**
15 h 50	**Sondage instantané – Deuxième séance**
16 h 05	**Table de discussion et dialogue**
16 h 45	**Que faire maintenant?** **Mot de la fin par l'honorable Denis Coderre**
17 h	**Clôture du forum**

ANNEXE III : PARTICIPANT(E)S INSCRIT(E)S (AU 6 OCTOBRE 2003)

Hon. Denis Coderre, C.P., député
Ministre, Citoyenneté et Immigration Canada

Diane Ablonczy
Députée, Calgary-Nose Hill

Reg Alcock
Député, Winnipeg Sud

Ken Anderson
Bureau de la Commissaire à l'information et à la protection de la vie privée de l'Ontario

Jahanshah Assadi
Délégation du Haut-Commissariat aux réfugiés pour le Canada

Sarkis Assadourian
Député, Brampton Centre

Rivka Augenfeld
Table de concertation des organismes au service des personnes réfugiées et immigrantes

Bill Bergen
Association canadienne de la technologie de l'information

Fariborz Birjandian
Alberta Association of Immigrant Serving Agencies

James Bissett
Commentateur des politiques

Anu Bose, Ph.D.
Organisation nationale des femmes immigrantes et des femmes appartenant à une minorité visible au Canada

Sam Boutziouvis
Conseil canadien des chefs d'entreprise

Robert Bouvier
Teamsters Canada

Brion Brandt
Transports Canada

Patrice Brunet
Association québécoise des avocats et avocates en droit de l'immigration

John Bryden
Député, Ancaster-Dundas-Flamborough-Aldershot

Mike Buisson
Gendarmerie royale du Canada

Rose Bullock
Alberta Government Services

Tony Cannavino
Association canadienne de la police professionnelle

Marc-André Charlebois
Association canadienne des agences de voyages

Anna Chiappa
Conseil ethnoculturel du Canada

Peter Clark
Conseil canadien des normes

Prof. Andrew Clement
Faculty of Information Studies, University of Toronto

Graham Cooper
Alliance canadienne du camionnage

Irwin Cotler
Député, Mont-Royal

Michelle d'Auray
Secrétariat du Conseil du Trésor

Madeleine Dalphond-Guiral
Députée, Laval-Centre

Raymond D'Aoust
Commissariat à la protection de la vie privée du Canada

Bob Davidson
Association du transport aérien international

Michel d'Avignon
Solliciteur général du Canada

Janet Dench
Conseil canadien pour les réfugiés

Prof. Alan M. Dershowitz
Harvard Law School

Bonnie Diamond
Association nationale de la femme et du droit

Michel Dorais
Citoyenneté et Immigration Canada

Roland Dorsay
Conseil des aéroports du Canada

Ward Elcock
Service canadien du renseignement de sécurité

Barry Elliott
Police provinciale de l'Ontario

Warren Everson
Association canadienne du transport aérien

David Flaherty, Ph.D.
David H. Flaherty Inc., Privacy and Information Policy Consultants

Jean-Guy Fleury
Commission de l'immigration et du statut de réfugié du Canada

Raymonde Folco
Députée, Laval-Ouest

Joe Fontana
Député, London Centre-Nord

Bridget Foster
Atlantic Regional Association of Immigrant Serving Agencies

Roger Gibbins, Ph.D.
Canada West Foundation

Martin Giles
Service d'immigration du Royaume-Uni

Frank Graves
Les Associés de recherche EKOS Inc.

Roy Gray
Ministère des Affaires indiennes et du Nord Canada

Art Hanger
Député, Calgary-Nord-Est

Jonathan Hatwell
Délégation de la commission européenne au Canada

Ryan Higgitt
Étudiant

Peter Hope-Tindall
dataPrivacy Partners Ltd.

Martin Huddart
International Biometric Industry Association

Thelma Johnson
Conseil de la statistique de l'état civil du Canada

Catherine Johnston
Association canadienne de la technologie des cartes à mémoire vision ACT

Onno Kremers
Développement des ressources humaines Canada

François Laporte
Teamsters Canada

John Lawford
Public Interest Advocacy Centre

Anne Legars
Fédération maritime du Canada

Sophia Leung
Députée, Vancouver-Kingsway

Alfred MacLeod
Citoyenneté et Immigration Canada

Inky Mark
Député, Dauphin-Swan River

Robert Marleau
Bureau du Commissaire à la vie privée du Canada

Robert Martel
Inuit Tapiriit Kanatami

Gordon Maynard
Association du barreau canadien

Kathryn McCallion
Ministère des Affaires étrangères et du Commerce international

Steve McCammon
Association canadienne des libertés civiles

Gary McDonald
Ministère des Affaires étrangères et du Commerce international

Kevin McGarr
Administration canadienne de la sûreté du transport aérien

Paul McGrath
Association des banquiers canadiens

Michael N. Murphy
Chambre de commerce du Canada

Raj Nanavati
International Biometrics Group, LLC

W. Russell Neuman, Ph.D.
Maison blanche

Massimo Pacetti
Député, St-Léonard-St-Michel

David Paterson
Alliance CATA

Chantal Péan
Commission canadienne du tourisme

Bill Pentney
Citoyenneté et Immigration Canada

Stephanie Perrin
Société Discrétion digitale Inc.

Thao Pham
Bureau du Conseil privé

Jim Phillips
CAN/AM Border Trade Alliance

Jerry Pickard
Député, Chatham-Kent-Essex

David Price
Député, Compton-Stanstead

Yves Prud-Homme
Fédération des policiers et policières municipaux du Québec

James Puleo
Organisation internationale des migrations

Hon. Robert K. Rae, C.P., O.C., C.R.
Goodmans LLP

Raj Rasalingam
Institut Pearson-Shoyama

Glenn Robinson
Bureau du Conseil privé

Gillian Russell
Commission européenne

Gerry Salembier
Ministère des Finances du Canada

Ravi Sall
Citoyenneté et Immigration Canada (Réseau des jeunes)

Marc Saner, Ph.D.
Institut sur la gouvernance

Colin Soutar, Ph.D.
Bioscrypt Inc./Alliance CATA

Johanne St-Cyr
Conseil canadien des administrateurs en transport motorisé

Valerie Steeves
Carleton University

Jennifer Stoddart
Commission d'accès à l'information du Québec

Tamy Superle
Étudiante

Roch Tassé
Coalition pour la surveillance internationale des libertés civiles

Maureen Tracy
Agence des douanes et du revenu du Canada

Gerry Van Kessel
Consultations intergouvernementales sur le droit d'asile, les réfugiés et les migrants

Sandi Villeneuve
Association des courtiers et intervenants frontaliers internationaux

Diane Vincent
Citoyenneté et Immigration Canada

Venita Warren
Citoyenneté et Immigration Canada (Réseau des jeunes)

Robert Whitelaw
Conseil canadien des bureaux d'éthique commerciale

Randy Williams
Association de l'industrie touristique du Canada

Patricia Woroch
Immigration Services Society

Lynne Yelich
Députée, Blackstrap

Elia Zureik, Ph.D.
Queen's University

ANNEXE IV : TABLE DE DISCUSSION ET DE DIALOGUE

À la fin de la réunion d'experts, les participants se sont vus accorder environ quarante-cinq minutes pour discuter de plusieurs questions clés avec les participants de leur table. Cette partie du rapport a pour objet de faire état du compte rendu présenté quant aux discussions ainsi que des commentaires inscrits dans des cahiers de travail par les participants de chaque table.

***Question 1** : Il est généralement admis que la protection de la vie privée constitue une préoccupation fondamentale lorsqu'il faut envisager des changements visant à améliorer l'intégrité de nos documents. Si des caractéristiques biométriques étaient adoptées dans le cadre de mesures visant à améliorer l'intégrité des documents*

- ***quelles mesures devraient être mises en oeuvre dans le but de veiller à la protection adéquate de la vie privée?***
- ***est-ce que les mesures existantes en matière de protection de la vie privée (loi, politiques, institutions) seraient suffisantes pour nous permettre de composer avec l'introduction d'identificateurs biométriques?***
- ***quel serait le rôle de la technologie en ce qui concerne la réalisation de vérifications appropriées et l'atteinte d'un juste équilibre?***

En réponse à la première question, les participants ont dégagé les mesures suivantes :

- Les limites à imposer quant à l'élargissement de la portée du projet.
- Les mesures de protection appropriées pour les données biométriques.
- Une fonction de supervision indépendante fondée sur la loi.
- Une clarté et une transparence quant aux objectifs et aux processus liés aux systèmes.

En ce qui a trait aux mesures de sécurité existantes en matière de protection de la vie privée, les participants étaient d'avis que :

- Il n'existe actuellement pas assez de mesures de sécurité pour empêcher l'utilisation non autorisée des données biométriques par le secteur privé.
- Un meilleur cadre de reddition de compte doit être mis en oeuvre.

Enfin, les participants étaient d'avis que la technologie pourrait jouer de nombreux rôles. Elle pourrait fournir :

- une capacité de vérification;
- des dispositifs de résistance à la contrefaçon et à la manipulation requis pour certaines fonctions.

Question 2 : *Un document comportant des caractéristiques biométriques peut être mis en oeuvre dans le cadre de programmes à enregistrement volontaire ou obligatoire. Dans la mesure où l'objectif visé par l'initiative liée à l'intégrité des documents est la production de meilleurs documents plus sécuritaires qui sont plus sécuritaires du point de vue de la contrefaçon et du vol d'identité, un grand nombre de personnes croient qu'il faut que l'enregistrement soit obligatoire. D'un autre côté, cependant, les préoccupations relatives à la protection de la vie privée indiquent que les gens doivent pouvoir décider si oui ou non ils désirent que certaines de leurs caractéristiques biométriques apparaissent sur un document ou dans une base de données. Qu'en pensez-vous ?*

Les participants étaient d'avis que la mise en oeuvre de toute carte d'identité nationale comporte des répercussions importantes pour la vie privée, et cela, que l'enregistrement soit obligatoire ou non. Ils croyaient qu'une analyse de rentabilisation devrait être réalisée pour la mise en oeuvre d'une carte d'identité nationale, en se fondant sur la comparaison des coûts et des avantages par rapport aux solutions relatives à l'intégrité des documents. Il faudra aussi discuter davantage de l'objectif fondamental visé par la mise en oeuvre de la carte.

Certains participants ont indiqué qu'à leur avis, il était prématuré de se poser cette question étant donné que le gouvernement n'a pas encore décidé à quelles fins la carte sera utilisée. Les participants se sont aussi dit préoccupés du fait que les fonctions liées aux cartes pourraient éventuellement être confiées à des entrepreneurs, et des défis que cela risque de créer. Enfin, les participants se sont dit inquiets du fait que l'utilisation d'une carte d'identité nationale risque de s'étendre à des fins qui n'auraient pas été prévues à l'origine.

Question 3 : *Les intervenants du milieu actuel de la sécurité internationale et de l'exécution de la loi se préoccupent de l'intégrité des documents dans le contexte des voyages et des mouvements internationaux de personnes. Un certain nombre d'administrations (y compris la plupart des principaux partenaires commerciaux du Canada – les États-Unis, la Communauté européenne, etc.) et des organisations internationales ont pris des mesures visant l'introduction de caractéristiques biométriques dans les documents de voyage au cours des deux ou trois prochaines années :*

- ***Comment le Canada devrait-il réagir face à ces développements?***
- ***De quelle latitude le Canada dispose-t-il pour agir de façon indépendante quant à cette problématique?***

Un certain nombre de participants ont voulu savoir pourquoi nous préconisons l'utilisation de la biométrie en tant que réponse à une question qui n'est pas bien comprise. Ces participants ont demandé si le Canada avait écarté d'autres approches comme l'élaboration de papiers d'identité sécuritaires. D'autres participants voyaient quant à eux la nécessité de concevoir une telle carte dans le but de suivre le rythme imposé par nos principaux partenaires commerciaux. Les initiatives à explorer suggérées par les participants comprenaient l'examen de documents de voyage, la participation aux activités d'organes de normalisation ainsi que d'autres activités visant à nous permettre de modeler les résultats des discussions internationales sur les normes et les priorités de façon à ce qu'ils correspondent aux valeurs collectives des Canadiens. Les participants ont indiqué que si le Canada devait se lancer dans de telles initiatives, il devrait trouver des partenaires ayant la même vision des choses que lui, et travailler avec eux à l'élaboration de normes internationales efficaces.

D'autres participants ont indiqué que toute une série de questions relatives à la mise en oeuvre d'une carte d'identité nationale n'étaient pas traitées dans le cadre de la conférence. Voici quelques-unes de ces questions :

- le système d'enregistrement;
- les répercussions sur les échanges commerciaux, qu'elles soient positives ou négatives;
- l'accès à d'autres masses continentales;
- la souveraineté;
- le sens de l'éthique et la dignité;
- la révocation;
- est-ce qu'il y a un plan B dans le cas où les choses ne tourneraient pas rond, un genre de scénario de ce qui pourrait arriver de pire?

ANNEXE V : SOMMAIRE DU DOCUMENT D'INFORMATION DU FORUM DES POLITIQUES PUBLIQUES

À la demande de Citoyenneté et Immigration Canada, le Forum des politiques publiques a rédigé un document d'information en vue du forum sur la biométrie. La présente annexe fournit un survol de ce document d'information. Le texte intégral du document d'information et d'autres documents liés au forum sur la biométrie sont disponibles sur le site Web créé spécialement par CIC en vue du forum : **http://cic-forum.ca/francais/default.asp.**

Les points clés examinés en ce qui a trait à l'utilisation possible des données biométriques abordés dans le document comprennent :

1) Applications

- *Identification et vérification*

2) Types de données biométriques

- *Caractéristiques physiologiques et caractéristiques comportementales*

3) Utilisations, y compris :

- *Emmagasinage dans une puce d'ordinateur*
- *Encodage sur une carte d'identité nationale*
- *Utilisation dans les contextes de la citoyenneté, de l'immigration et des voyages*

4) Mesure du rendement

- *Taux de refus erroné*
- *Taux de fausse reconnaissance*

Le document d'information suggérait aussi un certain nombre de questions clés à examiner dans un contexte de politique publique :

1) Juste équilibre entre sécurité, protection de la vie privée et libertés fondamentales

- *Sur quelles valeurs fondamentales devraient se fonder les décisions concernant l'utilisation de la biométrie dans les documents d'identité relatifs à la citoyenneté ou à l'immigration?*
- *La relation entre ces valeurs équivaut-elle à un jeu à somme nulle?Par exemple, une protection accrue de la vie privée se fera-t-elle nécessairement au détriment de la sécurité (ou vice versa)?*

2) Finalité et application

- *Quels objectifs d'intérêt public l'utilisation de la biométrie dans les documents de citoyenneté et d'immigration permettra-t-elle d'atteindre?*
- *Quelles applications(identification ou vérification) seraient utilisées*

3) Technologie au service de la protection de la vie privée et gestion de l'information

- *Existe-t-il des technologies qui peuvent garantir une protection adéquate de la vie privée et des renseignements personnels?*
- *Quelles bases de données gouvernementales seraient liées à des documents biométriques? Comment l'information serait-elle gérée?*

4) Faisabilité

- *La technologie est-elle au point et peut-elle répondre aux attentes?*
- *Y a-t-il des technologies, ou des combinaisons de technologies, qui devraient être privilégiées? Exclues*

5) La biométrie et la loi

- *Le cadre juridique actuel est-il approprié? Quels ajustements faudrait-il apporter?*
- *Est-il applicable?*

6) La gestion publique

- *Est-il possible d'adopter une approche nationale unique? Ou vaut-il mieux que chaque ordre de gouvernement ou chaque programme ait son approche particulière?*
- *Les mécanismes politiques et juridiques de surveillance et de reddition de compte sont-ils appropriés? Ou faut-il en créer d'autres?*
- *Dans quelle mesure est-ce qu'il importe d'harmoniser la conception et l'exécution à l'échelle internationale*

7) La capacité financière et administrative

- *Du point de vue financier et administratif, est-il faisable d'instaurer des documents de citoyenneté et d'immigration biométriques?*

8) Les documents biométriques : un système cohérent

- *À quoi ressemblerait un système biométrique efficace dans les domaines de la citoyenneté et de l'immigration?*
- *Les documents que ce système comporterait seraient-ils obligatoires? Dans l'affirmative, leur mise en oeuvre pourrait-elle reposer sur le principe du respect volontaire*

Le document d'information élaboré par le forum des politiques publiques est disponible à l'adresse suivante :

http://www.cic-forum.ca/francais/background_FR.pdf

Pour en obtenir une copie sur papier, veuillez communiquer avec le Forum des politiques publiques, à l'adresse suivante :

Forum des politiques publiques
1405 - 130 rue Albert
Ottawa (Ontario) K1P 5G4
Tél. : (613) 238-7160
Téléc. : (613) 238-7990

ANNEXE VI : SOMMAIRE DES RÉSULTATS DES SONDAGES INSTANTANÉS

Au début et à la fin de la deuxième journée de la séance, les participants se sont vus offrir l'occasion de fournir des commentaires instantanés sur un certain nombre de questions, au moyen de la technologie de Sharpe Decisions Inc. La présente annexe présente les résultats de ces sondages instantanés.

Première séance (matin de la deuxième journée du forum)

A) Dans quelle mesure est-ce important que le gouvernement du Canada aille de l'avant avec des mesures visant à améliorer l'intégrité de ses documents d'identité au cours des deux prochaines années

1	Pas important	3 %
2	Important	27 %
3	Très important	52 %
4	J'estime qu'il y a des priorités plus urgentes.	16 %

B) Compte tenu de votre opinion au sujet de l'importance d'améliorer l'intégrité des documents d'identité, êtes-vous en faveur

1	de l'adoption d'une approche plus globale, comme une carte d'identité nationale?	35 %
2	de l'adoption d'une approche plus progressive, comme l'amélioration de l'intégrité des documents existants (p. ex., passeport ou permis de conduire)?	48 %
3	du maintien du statu quo, tout en améliorant l'intégrité des documents primaires?	11 %
4	Je n'ai pas d'opinion..	4 %

C) Comment qualifieriez-vous votre niveau de connaissances de la biométrie

1	Très faible	3 %
2	Faible	25 %
3	Bon	50 %
4	Très bon	20 %

D) Laquelle des affirmations suivantes décrit le mieux vos intérêts à l'égard de ce forum?

1	Je travaille directement avec la biométrie.	12 %
2	Je m'intéresse aux diverses applications de la biométrie du point de vue technologique.	9 %
3	Je m'intéresse surtout aux répercussions sociales de la biométrie.	62 %
4	Je m'intéresse aux autres applications de la biométrie.	10 %
5	Je ne m'intéresse pas du tout à cette technologie.	0 %
6	Aucune de ces réponses.	4 %

E) Selon vous, l'utilisation frauduleuse des documents d'identité constitue-t-elle un problème sérieux au Canada?

1	Pas du tout sérieux	1 %
2	Pas très sérieux	3 %
3	Moyennement sérieux	21 %
4	Plutôt sérieux	25 %
5	Extrêmement sérieux	35 %
6	Ne sait pas/Aucune réponse	12 %

F) Personnellement, êtes-vous d'accord pour que le gouvernement fédéral ait recours à la biométrie pour réduire l'utilisation frauduleuse des documents d'identité?

1	Entièrement en désaccord	4 %
2	Plutôt en désaccord	17 %
3	Pas d'opinion	4 %
4	Plutôt d'accord	28 %
5	Entièrement d'accord	44 %

G) Compte tenu des préoccupations grandissantes au sujet de la vérification de l'identité des individus, quelle est selon vous la probabilité que presque tous les Canadiens adultes aient, d'ici la fin de la décennie, au moins un indicateur biométrique pour vérifier leur identité

1	Absolument improbable	1 %
2	Pas très probable	1 %
3	Plutôt probable	8 %
4	Très probable	83 %
5	Ne sait pas	5 %

Deuxième séance (après-midi de la deuxième journée du forum)

H) Compte tenu de l'utilisation grandissante de la biométrie par les secteurs public et privé, certaines personnes estiment que les gouvernements devraient réglementer l'utilisation, le stockage et l'échange de ce type de renseignements. Laquelle des affirmations suivantes reflète le mieux votre point de vue?

1	Les gouvernements devraient réglementer l'utilisation de la biométrie.	55 %
2	Il y a trop de risques associés à l'utilisation de la biométrie.	6 %
3	J'ai besoin de plus amples renseignements sur cette question.	38 %

I) Laquelle des affirmations suivantes reflète le mieux votre point de vue?

1	La biométrie offre la possibilité de réduire les revenus perdus (se chiffrant en millions de dollars) découlant de l'utilisation de documents d'identité frauduleux. Nous nous devons d'envisager sérieusement la possibilité de recourir à cette technologie.	51 %
2	Le crime organisé a recours à des moyens très avancés, notamment dans le domaine de la fabrication et du trafic de documents illégaux; ce n'est qu'une question de temps avant qu'il puisse contourner cette technologie.	25 %
3	Ne sait pas/Aucune réponse	23 %

J) Laquelle des affirmations suivantes reflète le mieux votre point de vue

1	Je pourrais accepter que l'on utilise la biométrie dans le contexte de la citoyenneté et de l'immigration si le gouvernement pouvait me prouver qu'il sera en mesure de protéger ces renseignements biométriques.	72 %
2	Comme il y a eu de nombreux exemples de situations où les gouvernements ont perdu des renseignements personnels secrets ou n'ont pas respecté les procédures de sécurité concernant ces renseignements, personne ne devrait être tenu de fournir ce type de renseignements personnels, les nouveaux arrivants au Canada non plus.	12 %
3	Ne sait pas/Aucune réponse	15 %

K) Laquelle des affirmations suivantes reflète le mieux votre point de vue

1	Des documents servant à établir l'identité sont perdus ou volés chaque jour. Si les renseignements biométriques tombaient entre les mains des mauvaises personnes, cela représenterait une menace encore plus grande pour la protection des renseignements personnels.	27 %
2	Il est de plus en plus facile de voler l'identité d'une personne. L'utilisation des technologies biométriques fera en sorte qu'il sera plus difficile pour les criminels de reproduire ou de contrefaire des documents d'identité existants et permettrait de mieux protéger les renseignements personnels.	62 %
3	Ne sais pas/Aucune réponse	9 %

L) Laquelle des affirmations suivantes reflète le mieux votre point de vue?

1	Il est logique de recourir à la biométrie, mais uniquement dans le cas des personnes pour lesquelles cette technologie représente des avantages, comme les voyageurs qui se soumettent à un lecteur de l'iris pour passer plus rapidement à travers les contrôles de sécurité dans les aéroports.	9 %
2	Sur le plan de la sécurité, les avantages découlant de l'utilisation de la biométrie n'existeraient plus si les renseignements biométriques étaient recueillis sur une base volontaire.	15 %
3	D'autres questions doivent être examinées avant de s'attaquer à la question de l'enregistrement obligatoire ou facultatif.	74 %

M) Laquelle des affirmations suivantes reflète le mieux votre point de vue?

1	Compte tenu de la situation à l'échelle internationale, toutes les personnes qui désirent venir au Canada, soit à titre de réfugié ou d'immigrant, devraient fournir des identificateurs biométriques avec leur demande.	36 %
2	Il serait injuste de cibler uniquement les nouveaux arrivants au Canada. L'utilisation de documents d'identité frauduleux est un problème qui se fait sentir un peu partout et qui nécessite une réponse plus globale.	54 %
3	Ne sait pas/Aucune réponse	9 %

N) Dans quelle mesure est-ce important que le gouvernement du Canada aille de l'avant avec des mesures visant à améliorer l'intégrité de ses documents d'identité au cours des deux prochaines années?

1	Pas important	0 %
2	Important	19 %
3	Très important	61 %
4	J'estime qu'il y a des priorités plus urgentes.	19 %

O) Compte tenu de votre opinion au sujet de l'importance d'améliorer l'intégrité des documents d'identité, êtes-vous en faveur :

1	de l'adoption d'une approche plus globale, comme une carte d'identité nationale?.	23 %
2	de l'adoption d'une approche plus progressiste, comme l'amélioration de l'intégrité des documents existants (p. ex., passeport ou permis de conduire).	56 %
3	du maintien du statu quo, tout en améliorant l'intégrité des documents primaires.	20 %
4	Je n'ai pas d'opinion.	0 %